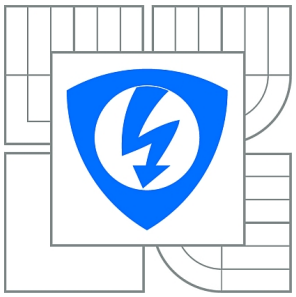
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

REALIZACE VOIP ÚSTŘEDNY ASTERISK

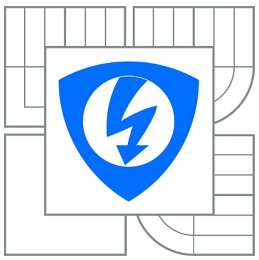
IMPLEMENTATION OF ASTERISK VOIP PBX

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MARTIN SCHÖN
AUTHOR

VEDOUCÍ PRÁCE — Ing. JURAJ SZŐCS
SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Martin Schön ***ID:*** 119601
Ročník: 3 ***Akademický rok:*** 2010/2011

NÁZEV TÉMATU:

Realizace VoIP ústředny Asterisk

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s používanými telekomunikačními protokoly VoIP, především s SIP, IAX, H.323, RTP a open-source pobočkovou telefonní ústřednou Asterisk. Prostudujte možnosti zabezpečení signalizace VoIP, přenosu RTP vůči odposlechům a samotné ústředny Asterisk vůči síťovým útokům. Popište jednotlivé audio/video kodeky, které nabízí PBX Asterisk a vyzkoušejte je na Vámi sestavené síti, kde budete testovat jejich náročnost na šířku pásma. Prozkoumejte jak velký vliv má šifrovaná a nešifrovaná komunikace na komunikační kanál. Součástí práce bude taky vytvoření dialplanu s demonstračními úlohami na IVR, přesměrování hovorů, překladu mezi protokoly SIP-H323 a SIP-SKYPE, integrací LDAP a oznamování příchozích hovorů pomocí protokolu XMPP.

DOPORUČENÁ LITERATURA:

[1] MEREL, D., DEMSPSTER, B., GOMILLION, D. Asterisk 1.6. Packt Publishing, 2009. 239 s. ISBN 978-1-847198-62-4.
[2] BOUCADAIR, M. Inter-Asterisk Exchange (IAX): Deployment Scenarios in SIP-Enabled Networks. John Wiley & Sons Ltd., 2009. 272 s. ISBN: 978-0-470-77072-6.

Termín zadání: 7.2.2011 ***Termín odevzdání:*** 2.6.2011

Vedoucí práce: Ing. Juraj Szőcs

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Bakalářská práce je rozdělena na dvě části, teoretickou a praktickou. V teoretické jsou rozebírány signalizační protokoly, protokol RTP pro přenos dat, VoIP ústředna Asterisk a jejich možnosti zabezpečení. V praktické části je popsána instalace ústředny Asterisk, provedena ukázka přesměrování hovorů. Ústředna byla spojena s adresářovým serverem LDAP pro správu uživatelů a Ejabberd pro zasílání textových zpráv protokolem XMPP. Dále byl nakonfigurován překlad SIP-SKYPE s využitím SiSky brány a pomocí dialplanu překlad SIP-H.323. Součástí práce bylo vypracování Dialplanu s IVR. Bylo změřeno zatížení šířky pásma audio/video kodeky při šifrovaném/nešifrovaném spojení.

KLÍČOVÁ SLOVA

VoIP, Asterisk, SIP, SKYPE, Zabezpečení, SRTP, LDAP, IVR, XMPP, Kodeky, Šířka pásma

ABSTRACT

The thesis is divided into two parts, theoretical and practical. In theory, it analyzed the signaling protocols, the RTP protocol for data transmission, VoIP Asterisk PBX and security options. The practical part describes the installation of the Asterisk PBX, conducted demonstration call forwarding. PBX was associated with an LDAP directory server to manage users and ejabberd for text messaging protocol XMPP. It was configured translation SIP-Skype using the SiSky Gateway and with dialplan SIP-H.323 translation. The study was to develop Dialplan with IVR. It was measured bandwidth of the audio/video codecs in an encrypted/unencrypted connections.

KEYWORDS

VoIP, Asterisk, SIP, SKYPE, Security, SRTP, LDAP, IVR, XMPP, Codecs, Bandwidth

SCHÖN, Martin *Realizace VoIP ústředny Asterisk*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2011. 64 s. Vedoucí práce byl Ing. Juraj Szőcs

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Realizace VoIP ústředny Asterisk“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

Brno ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

V dnešním moderním světě, kde se technika rozvíjí nezadržitelně rychle, se začíná do popředí propracovávat technologie VoIP. Podstata je sjednotit všechny služby telekomunikačního světa, podporovat staré, ale i využívat rozšíření internetové sítě. Internetové sítě pracují na odlišném principu oproti veřejné telefonní síti, které pracují na přepínání okruhu, a tím zaručují konstatní šířku pásma, zpoždění a jitter. Internet je založen na paketovém principu, tudíž nativně není zaručeno, že se paket s daty doručí příjemci. Dále zpoždění paketů, ztráta či přijetí paketů v nesprávném pořadí v paketově orientované síti není pro VoIP ideální. Proto se často s VoIP nasazují i síťové prvky s podporou QoS, která se snaží zajistit pro internetové volání či přenos videa, u kterého chceme zajistit odpovídající kvalitu, potřebné kapacity, a to potřebnou konstatní šířku pásma či priorizaci paketů dle služeb, což má za následek nejnižšího možného zpoždění s ideálně nulovým jitterem.

Při volání skrz internet může nastat problém s odposloucháváním hovorů, jelikož nativně jsou signalizační protokoly posílány v nešifrované podobě a kdokoliv si může zachytit dané pakety s daty o hovořících, ale dokonce i celý hovor, posílaný mezi účastníky protokolem RTP, si může po ukončeném volání přehrát. Další problém může být nezabezpečená signalizace hovorů, jelikož jejím zneužitím může útočník registrovat svůj telefon k ústředně a volat do zahraničí, což by pak firmu stálo nemalé peníze. Útočník nemusí útočit na koncové body, ale přímo na VoIP ústřednu a tedy ochromit veškerou komunikaci, kterou ústředna obsluhuje. Práce se bude právě v první části problematikou zabezpečení ve VoIP zabývat.

Dalším cílem bakalářské práce bude realizace ústředny, popis instalace na linuxovou distribuci Ubuntu server 11.04 při použití Asterisku verze 1.8.4.1 a propojení s dalšími službami LDAP, Skype a XMPP. Služby budou využívány v číslovacím plánu a vytvořen bude i jednoduchý interaktivní hlasový automat. Dále se práce zaměřuje na audio/video kodeky a jejich náročnost na šířku pásma v nešifrované a šifrované podobě.

1 PROTOKOLY VOIP

Volání přes Internet Protocol (IP) sítě vyžaduje protokoly, které vytvoří spojení mezi volajícím a volaným a přenáší multimediální data. Protokoly lze rozdělit na řídící a protokoly nesoucí užitečná data. Řídící můžeme nazvat taktéž signalizační a jejich úlohou v Voice over Internet Protocol (VoIP) je např. navázat spojení, ukončit spojení, zjistit zda-li je volaný dostupný a jeho funkce, které může využít k hovoru jako například audio, video. Nejčastěji se využívají následující signalizační protokoly, a to konkrétně H.323, Session Initiation Protocol (SIP), Inter-Asterisk eXchange (IAX/IAX2), o kterých se blíže dozvíte v následujících kapitolách. Pro vlastní přenos multimediálních dat využivají SIP a H.323 protokol Real-Time Transport Protocol (RTP). U IAX se používají Mini či Meta rámce, definovaný přímo v rámci IAX.

1.1 H.323

H.323 verze 1 byla vytvořena v roce 1996 sdružením International Telecommunications Union (ITU). Protokol se stále vyvíjí a současná verze 7 je z roku 2009. H.323 byl navržen pro real-time přenos audio, video či dat v paketově-orientovaných sítích bez podpory QoS. H.323 protokol zastřešuje i další, a to pro nás důležité signalizační protokoly – H.225.0 RAS (Registration, Admission, Status), H.225.0 Q.931 (hovorová signalizace), H.245 (řízení médií), dále protokoly pro přenos médií RTP/RTCP, protokoly pro kompresi audio (G.7xx) video (H.26x) či dat (T.120). Komponenty sítě H.323 pro přenos multimediálních dat jsou například telefony, video konferenční terminály, brány či vícebodové řídící jednotky. Všechny jmenované zařízení se řadí do skupiny koncových zařízení (endpoints). Odlišným zařízením od ostatních je gatekeeper, který nabízí své služby právě koncovým zařízením. H.323 síť se skládá z administrativních domén (administrative domains), kde v jedné administrativní zóně je maximálně jeden gatekeeper. V síti H.323 existují dva typy spojení point-to-point nebo multipoint konference. [1] [2]

1.1.1 Komponenty

Terminal (terminál)

Je koncové zařízení, které umožňuje v navázat komunikaci s jiným H.323 terminálem, bránou či MCU. Pokud terminál volá mimo svoji síť, využívá k tomu bránu. Obsahuje povinně systém control (signalizace), přenos multimedií, audio kodek a síťové rozhraní, volitelně video kodek a uživatelské aplikace. [1] [7]

Gateway (brána)

Slouží k navázání spojení mimo síť H.323, např. s PSTN, GSM či PBX. Brána se postará o konverzi multimediálních dat a signalizace, která slouží k řízení spojení mezi dvěma uživateli. [1] [7]

Multipoint Control Unit (vícebodová řídící jednotka)

MCU podporuje spojení 3 a více terminálů. Terminály se musí před samotnou konferencí spojit s MCU, která řídí veškerá spojení, nastavení kodeků i kdo bude hlavní řečník, což nastavuje podle síly hlasu nebo lze manuálně nastavit jeden terminál jako řečník. [1] [7]

Gatekeeper

Gatekeeper poskytuje adresní překlad (např. z E.164 na IP), řízení přístupu, autentifikaci, účtování, směrování a může i udávat šířku pásma terminálům, bránám či MCU. Ke komunikaci mezi koncovými zařízeními a gatekeeperem se používá H.225.0 RAS protokol. I přes množství nabízených služeb není tato komponenta v síti povinná. [1] [7]

1.1.2 Adresace

V H.323 síti musí mít každý terminál svoji unikátní identifikaci, aby bylo možné se s ním spojit a vytvořit tak multimediální přenos. [6]

E.164 Dialed Digits (číslování)

Číslování E.164 blíže popisuje standard ITU-T E.164, který definuje sérii čísel s doporučeným maximálním počtem 17, obsahující číslice 0-9. O přidělení v síti H.323 se stará administrátor. [6]

URL ID

Formát URL ID se skládá z prefixu h323: následujícím uživatelským jménem, dále zavináč a po něm část hostname, která může obsahovat IP adresu či doménové jméno zařízení. [6]

- h323:userA@testing.local
- h323:userB@192.168.10.2

H.323 ID

Je řetězec znaků zvaný alias, např. zasedačka123, michal. Jeho využití je nejčastěji v lokálních sítích. [6]

MobileUIM

Používá se v bezdrátových sítích 802.11. [6]

1.1.3 Protokoly

H.225.0-RAS (Registration, Adminission and Status)

RAS signalizace se používá u H.225.0 zpráv k provádění registrace, kontrole přístupu, nalezení gatekeeperu (GRQ), kontrole šířky pásma, zjištění stavu a rozpojení spojení mezi koncovými zařízeními (terminál, brána) a Gatekeeperem pomocí protokolu UDP. V sítích bez gatekeeperu se RAS signalizace nepoužívá. [1] [2] [7]

Hovorová signalizace H.225

Vychází ze specifikace využívané v ISDN a to Q.931. Hovorová signalizace slouží k sestavení/rozpojení či údržby spojení mezi dvěma koncovými body H.323 a komunikuje přes TCP port 1720. Hovorová signalizace se vytvoří ještě před založením řídícího kanálu H.245. V síti bez gatekeeperu hovorová signalizace vznikne mezi koncovými body zapojených do hovoru, pokud je v síti gatekeeper, přenáší se hovorová signalizace přes něj. V tabulce 1.1 naleznete nejpoužívanější zprávy. [1] [2] [7]

Tab. 1.1: Seznam zpráv v hovorové signalizaci H.225

Zpráva	**Popis**
Setup	Žádost o navázání spojení mezi koncovými zařízeními
Call Proceeding	Odpověď na žádost Setup, volaný zpracovává žádost
Alerting	Volaný je informován o příchozím hovoru
Connect	Volaný vyzvedl telefon a hovor je spojen
Release Complete	Zpráva o odpojení jednoho z účastníků hovoru (uzavření spojení)
Facility	Žádost/potvrzení doplňkových služeb, zda-li bude hovor přímo mezi terminály nebo přes gateekeeper

Řídící signalizace H.245

Řídící signalizace zajišťuje výměnu kontrolních zpráv pomocí protokolu TCP mezi koncovými zařízeními (end-to-end) pro řízení H.323 koncových bodů, vytváří logické kanály pro audio, video, data a řídící informace. Dále slouží pro dohodu kodeků mezi zařízeními. Stejně jako u hovorové signalizace, když je v síti gatekeeper, řídící signalizace se přenáší pomocí gatekeeperu, pokud není, H.245 probíhá mezi koncovými zařízeními. [1] [2] [7]

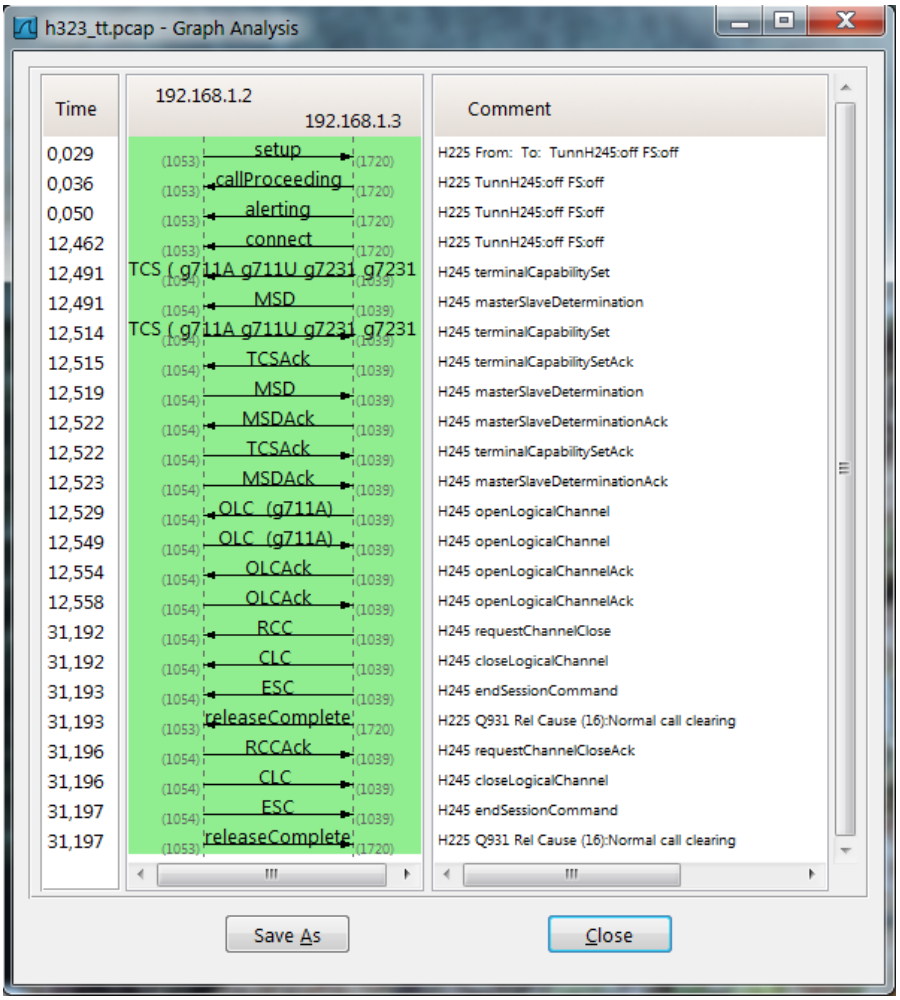
RTP a RTCP

První zmíněný poskytuje doručení na audio/video/data ke koncovým zařízením pomocí unicastu/multicastu. RTCP poskytuje řídící služby k protokolu RTP. Více informací o těchto dvou protokolech bude zmíněno na straně 23.

1.1.4 Signalizace

Terminál - Terminál

Nejdříve je nutné sestavení TCP spojení mezi terminály, které chtějí spolu komunikovat. Poté se posílá zpráva Setup, obsahující zdrojovou adresu a port volajícího, cílovou adresu a port volaného, typ volání, identifikaci spojení. Následuje Alerting (protistrana vyzvání) a pokud volaný vyzvedne sluchátko, je hovor přijat, odešle zprávu Connect a hovorová signalizace H.225 je dokončena. Poté přijde na řadu řídící signalizace H.245, která má na starosti vytvoření logického kanálu pro RTCP. To znamená výměnu IP adres a čísel portů, kterými bude řízeno posílání RTP paketů přenášejících multimediální data. Při zavěšení se vyšle zpráva Release Complete a ukončí se veškeré spojení mezi terminály. [15]



Obr. 1.1: Signalizace mezi terminály v síti H.323

1.2 SIP

Session Initiation Protocol je signalizační protokol vyvinutý pracovní skupinou IETF MMUSIC a je navržen pro navázání, upravování a ukončení spojení v IP sítích. Zahrnuje multimediální prvky jako jsou audio, video či IM. Původně byl vydán v roce 1996 jako RFC 2543 (zastaralý), nyní platí RFC 3261 [3]. Proti H.323 je výrazně jednodušší, jelikož SIP je textově orientovaný, vychází z protokolu HTTP a využívá i několik položek ze SMTP. [3] [4]

1.2.1 Komponenty

User Agents (UA)

User agent, neboli koncové zařízení je rozděleno na User Agent Client (UAC), zahrnující přenos média audio/video a User Agent Server (UAS), který například řídí tok dat. UAC inicializuje žádosti, zatímco UAS generuje odpovědi na přijaté žádosti. Každý user agent obsahuje UAC i UAS. UA může být hardwarový SIP telefon nebo klientský software s podporou protokolu SIP běžící např. na PC. User agent smí být i bránou do jiné sitě (např. do PSTN) a umožňovat tak volání/příjem hovoru do/z PSTN. [5]

Servers

V síti SIP probíhá signalizace na bázi klient-server, proto RFC 3261 [3] definuje 3 typy serverů, které nabízejí své služby user agentům.

Proxy server

Přijímá žádosti od UA nebo jiného proxy serveru a předává je ostatním proxy serverům, pokud volaného účastníka nezná. Proxy server se dělí na 2 typy: stateful a stateless. Stateful si pamatuje veškeré žádosti, a proto může zasahovat do hovoru, např. měnit šířku pásma. Stateless vyřídí žádost a dále se už spojením více nezabývá. Proxy server může obsahovat autentizaci, autorizaci, směrování a zabezpečení. [3] [6]

Redirect server

Při obdržení žádosti o navázání spojení vyhledá v databázi volajícího, zjistí, kde se volaný účastník nachází a vrací 3xx (přesměrování) s informacemi, na jakou URI má volající žádost zaslat. [3] [6]

Registrar server

Přijímá registrační žádosti od UAC a aktualizuje svojí databázi (URI s IP adresami) o UA, která jsou připojena v rámci domény. [3] [6]

1.2.2 Adresace

Standartní adresy (URI) používané v SIP začínají prefixem sip: a dále následuje adresa podobná emailové adrese. Příklady:

- sip:user@domena:port
- sip:clientA@testing.local
- sips:user@domena.cz:port
- sips:clientB@192.168.1.10

Prefix sips: definuje RFC 3261 [3] a zahrnuje zabezpečení, které využívá vzájemné ověření pomocí TLS. Port, pokud se používá defaultní 5060 (sips 5061) se psát nemusí, jinak musí být definován za adresou viz výše.

1.2.3 Komunikace v SIP

Jak bylo výše uvedeno, tak komunikace pomocí SIP protokolu je textového charakteru. V tabulce 1.2 je uvedeno pár metod (požadavků), které se nejčastěji používají při spojení. [5]

Tab. 1.2: Přehled metod v SIP

Metoda	**Popis**
INVITE	Žádost o zahájení relace
ACK	Potvzení na žádost INVITE
BYE	Ukončení spojení, při sestaveném spojení
CANCEL	Ukončení spojení, při nenavázaném spojení
REGISTER	Žádost o registraci zařízení s účastníkovým URI
OPTION	Dotaz na schopnosti UA

Formát odpovědí na metody je číslicový, vychází z HTTP a má 6 tříd, které jsou určovány první číslicí v kódu. [5]

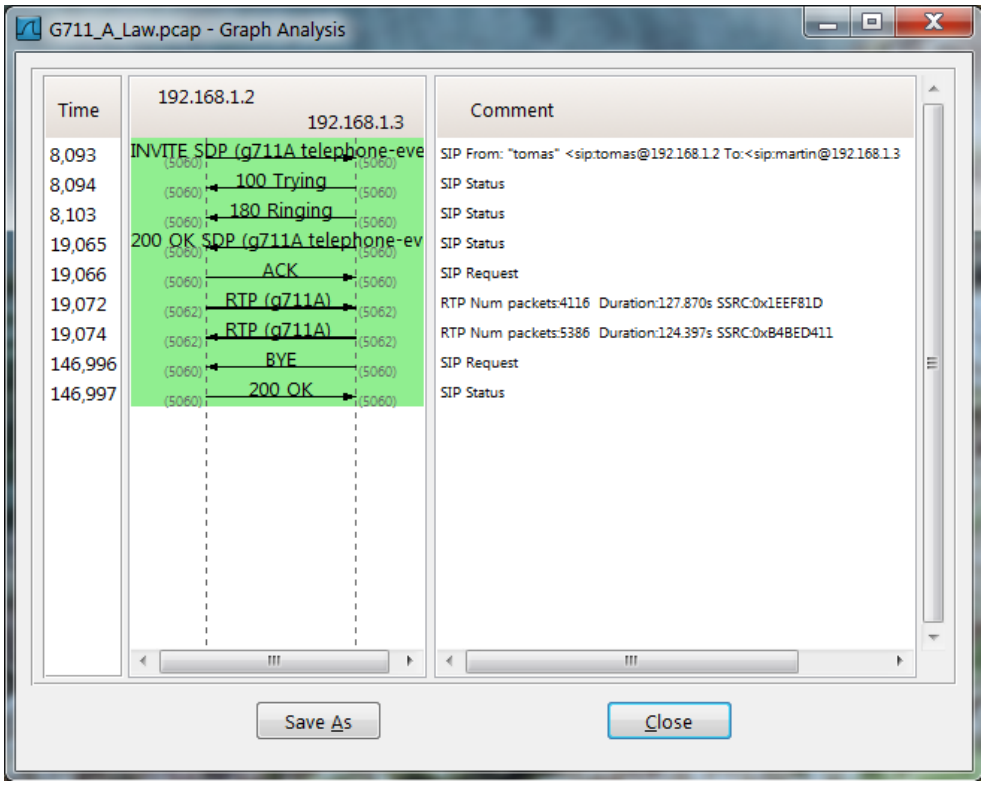
Tab. 1.3: Značení odpovědi SIP

Třída	**Popis**
1xx	Prozatimní nebo informační zprávy – požadavek pokračuje, neukončující relaci
2xx	Úspěch – Žádost byla úspěšně dokončena
3xx	Přesměrování – Žádost se musí vyslat na jiné místo
4xx	Chyba klienta – Žádost je chybná a nemůže být serverem zpracována
5xx	Chyba serveru – Žádost nebyla dokončena z důvodu chyby příjemce
6xx	Globání selhání – Žádost je chybná

1.2.4 Signalizace

Point to point

Žádost INVITE obsahuje s kým se chce volající spojit, pomocí jakého protokolu (v našem případě SIP verze 2). Na tuto žádost mu volaný odpoví informativní zprávou 100 Trying (nepovinná zpráva), že zpracovává žádost a poté vyšle zprávu 180 Ringing (protistrana vyzvání). Při vyzvednutí sluchátka posílá volaný UA zprávu 200 OK, kterou následně UA volající potvrdí ACK. Poté už je navázáno spojení a probíhá multimediální přenos audio/video dat. V případě zavěšení jednoho z účastníků, zašle jeho UA zprávu BYE s výzvou o uzavření spojení. Druhý účastník odesílá 200 OK a veškeré spojení zanikne. [6]



Obr. 1.2: Signalizace mezi dvěma UA

Pomocí proxy serveru

V tomto případě je veškerá signalizace směrována na proxy server, který přijme od volajícího UA žádost INVITE, do které přidá řádek via se svou adresou a pošle volanému UA. Dále je postup stejný jako v předchozím případě, až na zprávy 180 Ringing (protistrana vyzvání) a 200 OK (vyzvednutí sluchátka), které se přenáší přes proxy server. [6]

1.3 IAX

Vyvinut firmou Digium primárně na přenosy mezi Asterisk servery (PBX), ale může být použit i pro spojení server-klient. Protokol je otevřen pro kohokoliv a nikomu není bráněno vytvořit svoji VoIP ústřednu či VoIP klienta a protokol IAX využívat. V únoru roku 2010 vyšlo RFC 5456 [8], které definuje verzi 2. Výhoda oproti SIP a H.323 je použití jediného UDP portu přiděleným organizací IANA, a to port 4569 pro multimediální přenos, ale i signalizaci. To má za následek snižení počtu děr ve firewallu. Cílem protokolu je co nejmenší bandwidth, proto je protokol bineární z důvodu menší režie a tím více šířky pásma pro hovor(y). IAX protokol definuje vlastní rámce, ale i pro přenos užitečných dat. Pro signalizaci definuje, který jako jediný přijímací strana potvrzuje ACK. Pro přenos audio dat se používá Mini rámec nebo Full rámec. Další typ používaný v IAX je Meta rámec, který slouží pro přenos video dat či trunk linky. Každý typ rámce má i šifrovanou verzi. [8] [18]

1.3.1 Adresace

iax:[username@]host[:port][/number|name[?context]]

Username

Textový řetězec identifikující zařízení. Není povinná a jako jediná položka case sensitive.

Host:port

Obsahuje FQDN/IPv4/IPv6 adresu (IPv6 musí být v závorkách [2001:db8::1]) Číslo UDP portu, pokud je defaultní 4569, může se tato část vynechat, v opačném případě se musí napsat.

Number | name

Jméno nebo číslo, které identifikuje IAX hostitele. Tato položka není povinná.

Context

Název skupiny, v níž je IAX zařízení identifikováno. Nepovinné.

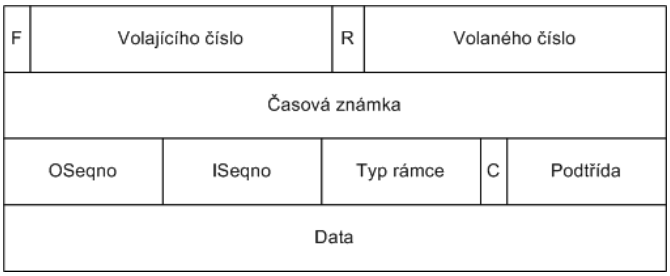
Příklady adres

iax:domena.cz:4569/honza
iax:[2002:db2::1]:4570/petr?kolega
iax:elvis@192.168.0.1/1242564571

1.3.2 Rámce

Full rámec

Jak už bylo výše zmíněno – Full rámec slouží k přenášení signalizace nebo multimediálních dat mezi účastníky hovoru. IAX využívá pouze jediného transportního protokolu (UDP), který je nespolehlivý, ale signalizační data je nutné s jistotou poslat druhé straně, je tento rámec potvrzován ACK protistranou. Struktura rámce je zobrazena na obrázku 1.3. [8] [18]



Obr. 1.3: Formát Full rámce

Mini rámec

Rámec používaný pro hlasová data, která je nutná urychleně přenést, proto je rámec odproštěn od nepotřebných informací, velikost časové známky je snížena na polovinu (16bit) a ani nemusí být potvrzován ACK protistranou. U hlasových rámců nám výpadek rámce citelně neovlivní hovor. Audio data jsou kódovány pomocí definovaného kodeku, domluveným mezi účastníky v předchozím Full rámci. Struktura rámce je zobrazena na obrázku 1.4. [8] [18]

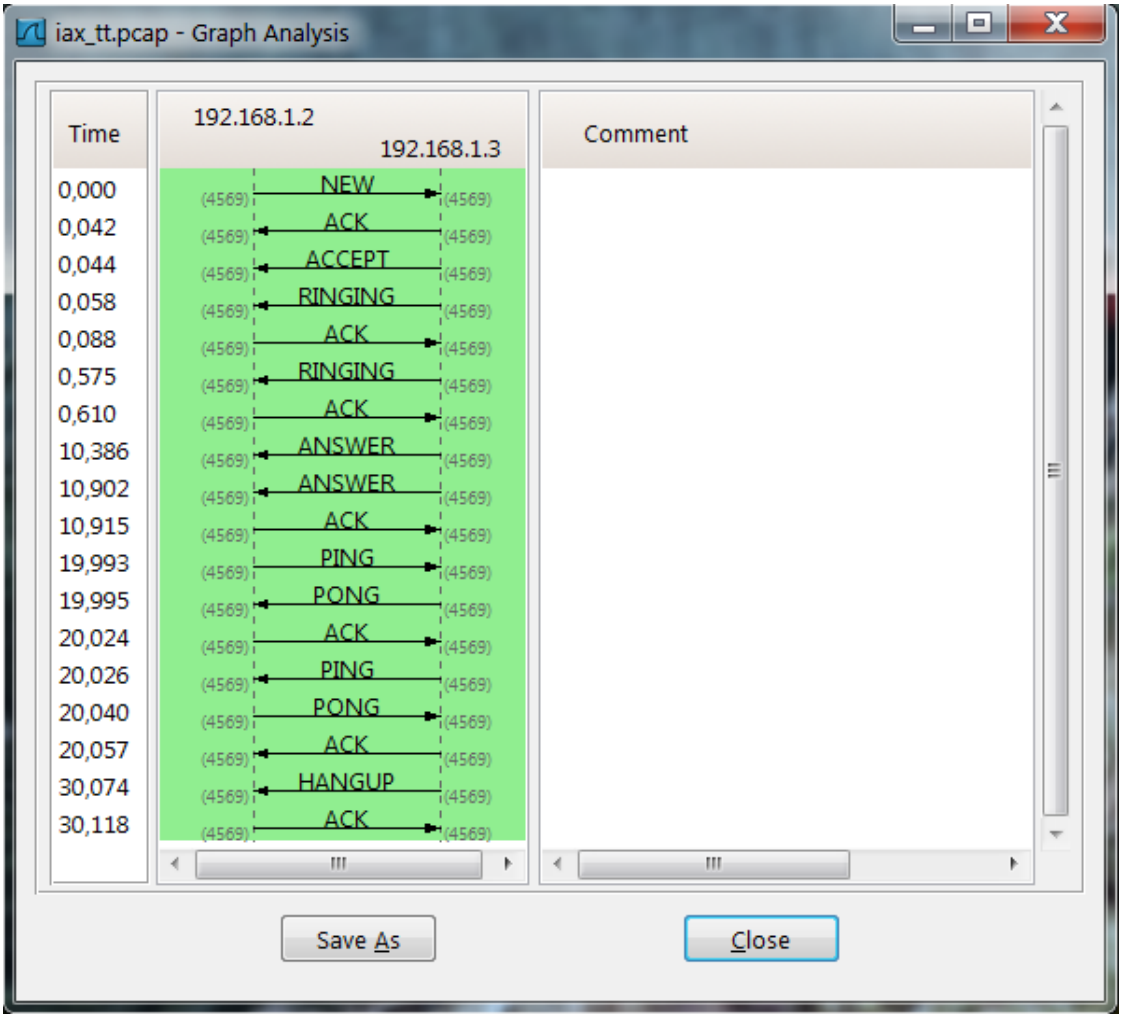
Obr. 1.4: Formát Mini rámce

Meta rámec

Rámec přenášející video data či pro trunk linku mezi PBX. Jeho hlavní výhoda nasazení v trunk linkách je při vícenásobném počtu hovorů přenášených mezi PBX, vnořuje informace o signalizaci pouze do jedné hlavičky, a tím zásadně šetří šířku pásma. [8] [18]

1.3.3 Signalizace

K sestavení hovoru mezi dvěma účastníky je zapotřebí vyměnit několik signalizačních zpráv. První zprávou je NEW, která přenáší informace o adresách. Volaný na zprávu odpoví ACCEPT, což znamená, že zprávu NEW přijal a zpracovává ji. Volající pošle ACK, tedy potvrzení zprávy ACCEPT. Dále je vyslán Full rámec, kvůli domluvení podporovaných služeb zařízení a synchronizaci, načež protistrana potvrdí ACK. Dále volaný pošle zprávu RINGING (protistrana vyzvání). V okamžiku přijetí hovoru volaným je odeslána zpráva ANSWER volajícímu a následuje hovor s Mini rámci přenášejícími audio data a Full rámci kvůli synchronizaci. Zprávy PING a PONG slouží k testování spojení mezi účastníky hovoru. [8] [18]



Obr. 1.5: Signalizace mezi dvěma IAX klienty

1.4 RTP

AVT (Audio/Video Transport) pracovní skupina pod organizací IETF vyvinula RTP v roce 1996 jako standard v RFC 1889. Vývoj dále postupoval a bylo nutné vydat další RFC 3550, které dále rozšířilo původní. Multimediální data se v reálném čase přenáší v paketové síti, nejčastěji internet, pomocí RTP (Real-Time Transport Protocol). K RTP se váže RTCP (RTP Control Protocol), který přenáší informace o RTP, a to statistiky paketů, kvalita přenosu, zpoždění paketů a synchronizace. RTP se přenáší pomocí UDP paketů, jelikož má nižší režii než TCP, u kterého se každý paket musí potvrzovat (ACK). V případě použití TCP a výpadku paketu by musel být paket znovu odeslán, a tím by narostlo zpoždění, což by negativně ovlivnilo komunikaci. Výpadek jednoho paketu hlasu/videa nikterak více neovlivní komunikaci. Signalizační protokol (H.323, SIP, IAX) předává RTP informace o UDP portech IP adresách a RTP zahájí obousměrný přenos multimediálního obsahu dle získaných informací. Každý typ dat (audio/video) musí mít svoje vlastní RTP spojení, výjimku tvoří DTMF (Dual Tone Multiple Frequency) definovaný RFC 2833, jež může použít stejné RTP spojení, a to pro DTMF číslice a hlasové pakety. Každé RTP spojení definováno IP adresou a číslem portu koncového bodu, IP adresou a číslem portu konferenčního serveru. Port na volaného zařízení se volí ze sudých čísel, o číslo vyšší port se používá pro RTCP. Struktura paketu RTP je popsána v tabulce 1.4. [6]

Tab. 1.4: Obsah paketu RTP

Část	**Popis**
Version (verze)	Identifikátor verze RTP protokolu, aktuální je 2
Payload type (typ dat)	Určuje kodek a vzorkovací kmitočet
Sequence Number (číslo sekvence)	Pořadové číslo vyslaného paketu, slouží příjemci ke kontrole, zda-li se nějaký paket neztratil při přenosu v síti.
Time stamp (časová známka)	Synchronizace a zpoždění
Synchronization Source Identifier (Identifikátor zdrojové synchronizace)	Identifikátor RTP spojení

2 ASTERISK

2.1 Obecně

Asterisk je open-source softwarová PBX běžící na platformách Linux. O její vznik roku 1999 se zasloužil Mark Spencer, který podle jeho slov neměl peníze na komerční produkt PBX ústředny a tak vytvořil svůj vlastní. Poslední verze 1.8 je ze dne 21. 10. 2010. Asterisk je obecná distribuce pod podmínkami GPL (General Public Licence), čili Asterisk je volně stáhnutelný z internetu a je možné zdrojové kódy upravovat k vlastní potřebě. Firma Digium dohlížející nad projektem Asterisk tedy neprofituje z vývoje ústředny, ale z její podpory a prodeje kompatibilního HW s ústřednou. Asterisk je ústředna spojující analogové sítě (PSTN) s paketově-orientovanými (IP, Frame relay) pomocí odlišných protokolů (SIP, H.323, IAX/IAX2, MGCP, SCCP). Dále nabízí IVR (Interactive Voice Response), jakožto hlasový terminál, který lze ovládat buď hlasem nebo tónovou volbou DTMF. Toho lze například využít při volání do firmy a slouží místo operátorky, kam chceme daný hovor přepojit, zda-li k technikům, mzdové účetní, řediteli či zanechat zprávu v hlasové poště. Veškerá nastavení je možné provádět pomocí textového editoru a příslušných souborů nebo také lze stáhnout z internetu upravené instalace s přidaným intuitivním webovým rozhraním, např. AsteriskNOW či Trixbox. [9] [10] [11]

Využití:

- Pobočková ústředna (PBX)
- VoIP brána pro různé protokoly (SIP, IAX/IAX2, H.323, MGCP, Skinny)
- Voicemail služby s adresářem
- Interaktivní hlasový průvodce IVR server
- Konferenční server
- Pro šifrování spojení
- Pro překlad čísel
- Pro systém předplacených volání
- Systém pro směrování cestou nejnižších nákladů (LCR)
- Centrum volání (Call Center)

2.2 Rozhraní

Jak již bylo výše uvedeno ústředna Asterisk dokáže obsluhovat hovory přicházející z analogové sítě. K tomu ale potřebuje rozšiřující hardware, jelikož dnešní servery obsahují pouze ethernet kartu, která slouží ke komunikaci v paketové síti. [9] [10]

2.2.1 Zaptel hardware

Původní TDM (Time-Division Multiplex) hardware byl patentovaný a velmi nákladný, proto se rozhodla firma Zapata Telephony vyrábět vlastní pseudo TDM rozhraní, tzv. Zaptel hardware. Vyznačoval se stejnou kvalitou a real-time zpracováním jako původní TDM hardware. Asterisk tedy nativně podporuje Zaptel hardware a firma Digium distribuje různé varianty (POTS, PSTN, E1, T1, PRI, PRA, atd.) [9] [10]

2.2.2 Non-Zaptel hardware

Hardware taktéž připojující ústřednu Asterisk s klasickou telefonní sítí, ale bez podpory pseudo TDM. Rozhraní (ISDN4Linux, OSS/Alsa, LTI - Linux Telephony Interface, Phonejack, Dialogic hardware). [9] [10]

2.2.3 Packet voice

Zaptel i Non-Zaptel hardware se zabývají připojením ústředny Asterisk k analogové síti, ke které potřebovali speciální hardware. K paketové síti (IP či Frame relay) žádný speciální hardware není potřeba. Asterisk má svůj vlastní protokol a to IAX, jenž přenáší signalizaci k sestavení hovoru i transport hlasových dat mezi komunikujícími stranami v paketové síti. Tvůrci ústředny ale nezůstali u jednoho protokolu, ale implementovali i další, často používané SIP, H.323, MGCP, Skinny/SCCP, aby vyhověli jakékoliv potřebě uživatele. [9] [10]

2.3 Podporované kodeky

Asterisk podporuje následující typy zvukových kodeků [12]

- a-law / μ-law
- G.722, G.726
- GSM
- iLBC (internet Low Bitrate Codec)
- MP3
- Speex

3 ZABEZPEČENÍ

Důležité je si uvědomit, že v základním nastavení je celý hovor (včetně signalizace) přenášen v nešifrované podobě. Útočník si může odchytit naši komunikaci a zpětně si ji přehrát (tzv. relay attack), kde si může poslechnout například firemní know-how nebo ostatní citlivé či tajné informace. Dále může odchytit autentizační hesla a využít tak naší ústředny pro hovory do zahraničí. Eavedropping útok, který je těžko odhalitelný, jelikož jde o přesměrování komunikace k útočníkovi, který sleduje průběh komunikace a dále jí přeposílá k volanému. Každý protokol sloužící ve VoIP má možnost nastavení různých zabezpečení. Dále je nutné zabezpečit i PBX ústřednu, jelikož i ona bývá terčem útoku, a protože je důležitým prvkem ve VoIP, je nutné se zabývat jejím zabezpečením. Nejčastější útoky a zabezpečení proti nim je uvedeno v dalších podkapitolách.

3.1 Signalizace VoIP

3.1.1 H.323

Jak už bylo řečeno H.323 sdružuje více protokolů a jedním z nich je H.235, který má na starosti bezpečnost. Ta je definována pomocí profilů, které umožňují nastavovat úrovně zabezpečení.

Baseline security profile

Baseline bezpečnostní profil využívá symetrické techniky. Sdílený klíč musí být zadán na obou stranách komunikace (endpoint, gatekeeper), což může být administrativně náročné ve velkých firmách. Klíč se používá ke kontrole autentizace či integrity zprávy. Pro přenos hesla a ověření se používá hashovací algoritmus HMAC-SHA-1. [15]

Signature security profile

Profil definuje doporučení zabezpečení signalizace pomocí SHA1, MD5 nebo digitálních certifikátů. Jelikož každá zpráva vyžaduje generování elektronického podpisu, je tento profil značně náročný na výkon, tudíž se zvyšuje latence. [15] MD5 byl prolomen a SHA1 taktéž není považován jako bezpečný hashovací algoritmus, není doporučeno je používat.

Hybrid security profile

Hybrid profil je kombinací Baseline security profile a Signature security profile, tedy využívá asymetrické (digitální certifikáty) i symetrické techniky (hash SHA-1). Princip je takový, že při prvotním navázání spojení je využito certifikátu, ve kterém se přenese i sdílené heslo a další zprávy jsou již zabezpečeny symetricky právě přeneseným sdíleným heslem. [15]

Voice encryption security profile

Tento profil zajišťuje šifrování hlasového obsahu paketů RTP. Definuje výměnu hlavního hesla pomocí hovorové signalizace H.225.0. Generování a distribuci media stream klíče pomocí řízení hovoru H.245. Poskytuje autentizaci a integritu RTP paketů výpočtem MAC (Message Authentication Code). Používá algoritmy DES, který byl prolomen, proto se doporučuje spíše využít SHA-1. Lze jej kombinovat s jakýmkoliv předešlým profilem. [15]

3.1.2 SIP

HTTP autentizace

Existují dva typy, a to základní, který ověřuje uživatele podle uživatelského jména a hesla. Identifikační údaje posílá sítí nezašifrovaně, tedy pouze jako snadno odchytitelný plain text. Druhý typ HTTP autentizace je rozšířený, který také využívá uživatelské jméno a heslo, ale sítí posílá jeho hash pomocí MD5 algoritmu. Jelikož bylo MD5 prolomeno, RFC 3261 nedoporučuje používat HTTP autentizaci. [15]

SIPS URI (TLS)

RFC 3261 doporučuje použití TLS na user agent server, proxy, redirect, registrars servrech k zabezpečení SIP signalizace. Dokáže chránit signalizaci proti ztrátě integrity, důvěrnosti. TLS spravuje klíče k vzájemnému ověření a bezpečnému přenosu klíče mezi zařízeními. Nevýhodou TLS je neschopnost zabezpečit UDP signalizaci. Stejně jako u HTTP je označení zabezpečeného přenosu přidáním písmena s na konec prefixu, tedy u SIP signalizace je sips. [15] TLS není použito end-to-end, ale mezi zařízeními neboli hop-by-hop. To znamená, že každý prvek, který je potřeba k spojení hovoru i UA musí mít podporu TLS zabezpečení. Princip TLS využívající certifikátů spočívá, že na začátku komunikace je nutné se domluvit na algoritmu. Poté se autentizují strany pomocí veřejného certifikátu. Dále už komunikují zašifrovaně pomocí symetrického algoritmu AES. [13]

Secure MINE (S/MIME)

SIP je přenášen end-to-end pomocí MIME zpráv. MIME zahrnuje mechanizmy pro autentizaci, zajištění integrity a důvěrnosti zpráv signalizačních dat. K zašifrování a podpisu zpráv S/MIME vyžaduje certifikáty a soukromé klíče, které byly vytvořeny důvěryhodnou třetí stranou (CA). Další možnost je vytvoření certifikátu zařízením, ale jelikož není označen za důvěryhodný, nemusí být jeho zprávy zpracovány. [15]

IP Security (IPsec)

IPsec pracuje na 3. vrstvě referenčního modelu ISO OSI, kde zajišťuje bezpečnost SIP signalizace. IPsec vytvoří zabezpečený kanál, kterým prochází signalizační i multimediální data. IPsec lze použít stejně jako u předchozího hop-by-hop, ale navíc i umožňuje end-to-end zabezpečení komunikace. IKE (Internet Key Exchange) hybridní protokol na správu klíčů založený na ISAKMP (Internet Security Association and Key Management Protocol) poskytuje automatickou výměnu šifrovacích klíčů a správu IPsec. [15]

3.1.3 IAX

IAX nativně podporuje šifrování signalizace i multimediálních zpráv pomocí algoritmu AES (Advanced Encryption Standard). Rijndael neboli AES je 128-bitová bloková šifra využívající stejného klíče na zašifrování/dešifrování dat. IAX šifruje každý hovor zvlášť (call-by-call). Při posílání první zprávy NEW jsou uvnitř informace o šifrování (ENCRYPTION IE) a pokud bude volaného zařízení schopno šifrovat, pošle nezašifrovaně zprávu AUTHREQ, do které také zahrne informace o šifrování (ENCRYPTION IE). Všechny další zprávy mezi zařízeními musí být šifrovány. Pokud volaný nepodporuje šifrování, tak do zprávy AUTHREQ nezahrne informace o šifrování a volající může buď ukončit hovor a nebo pokračovat s tím, že nebude šifrován. Klíč, který je používán v komunikaci je spojením CHALLENGE IE v AUTHREQ zprávě se sdíleným heslem. Klíč je po celou dobu hovoru stejný a šifruje se pouze část s daty. [8]

Rámce

Ještě před vlastním zašifrování Full rámce musí být přidána 128 výplň (padding), jelikož AES vyžaduje bloky dat po 128bitech. Výsledný Full rámec je zobrazen na obrázku 3.1. Lze vidět, že prvních 32bitů je nezašifrovaných. U Mini rámce je situace obdobná, jenom nezašifrovaných prvních bitů je 16. [8]

Full rámec

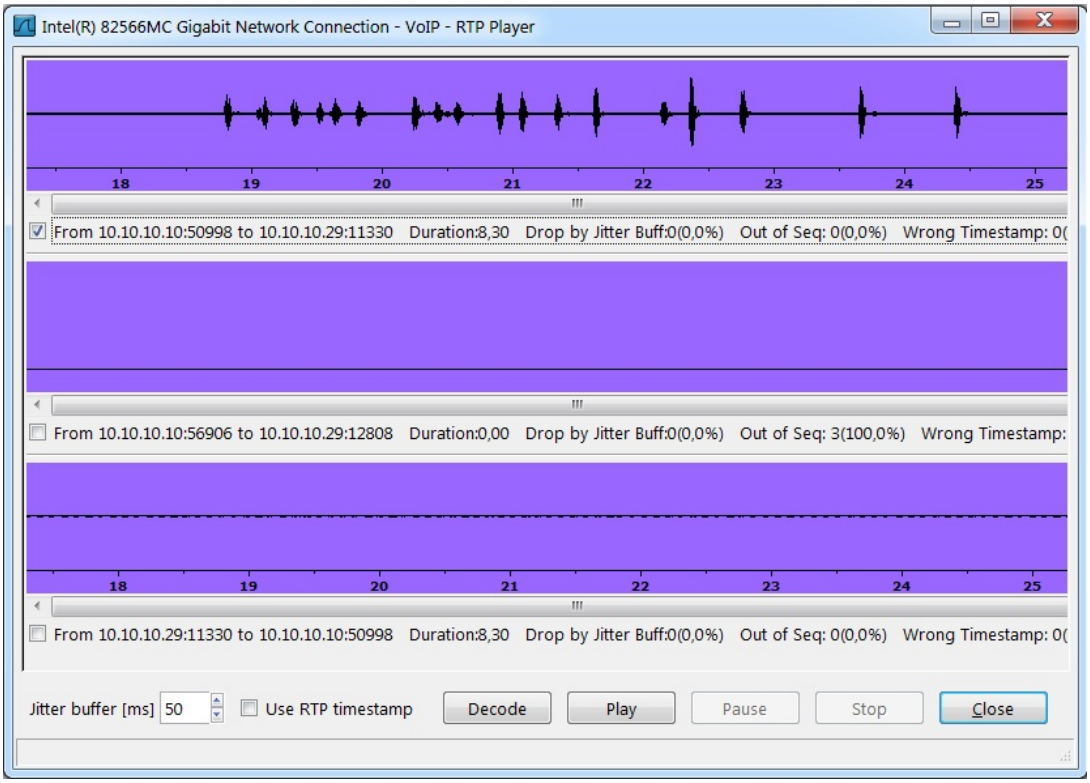
Obr. 3.1: Zašifrovaný formát Full rámec

Mini rámec

Obr. 3.2: Zašifrovaný formát Mini rámec

3.2 RTP vůči útokům

RTP využívají protokoly H.323 a SIP k přenosu multimediálního přenosu (audio/video). Je to nezabezpečený protokol a útočníkovi stačí pouze odchytit RTP pakety a dekódovat jejich obsah. Program Wireshark, který je volně ke stažení z internetu, slouží k zachytávání paketů na síťovém rozhraní, obsahuje právě možnost vytvoření filtru RTP paketů a následné přehrání multimediálních dat viz obrázek 3.3. Vzniklou situaci lze vyřešit nasazením SRTP, který obsahuje šifrování a více o něm je popsáno v další podkapitole.

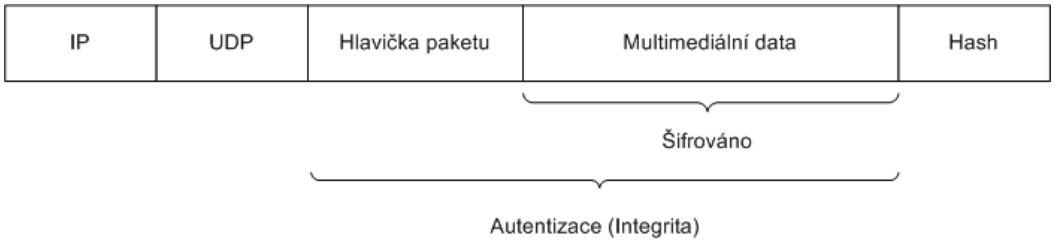


Obr. 3.3: Zachycený RTP pakety, kde hovoří pouze volaný

3.2.1 SRTP

Secure RTP je definován RFC 3711 [14] z roku 2004 a oproti RTP se jedná o šifrovaný RTP přenos dat, ale zajišťuje i integritu a autentičnost dat. Zašifrována jsou pouze multimediální data, nikoliv hlavička, a to z důvodu směrování paketů v síti a bez znalosti, kam poslat paket, není možné doručit příjemci data. Hlavička je zabezpečena pomocí hashovacího algoritmu SHA1. Princip je takový, že vysílací zařízení vezme paket a pomocí SHA1 vytvoří hash (otisk) z hlavičky a multimediálních dat.

Vytvořenou hash přidá na konec paketu. Přijimací zařízení přijme paket a vypočítá taktéž hash z přijaté hlavičky a dat. Tu porovná s přijatou hashí, která byla na konci paketu a pokud se obě hashe shodují, paket je prohlášen za původní odeslaný, tedy nebyl v průběhu přenosu nijak upravován. k šifrování multimediálních dat se využívá šifrovací algoritmus AES. [13] [14]



Obr. 3.4: SRTP paket

3.2.2 ZRTP & Zfone

SRTP je šifrováno AES symetrickým klíčem, tudíž je nutné mít stejný klíč na obou stranách. K jeho přenosu se využívá signalizační protokol SIP/H.323, ale pokud je např. SIP přenášen v nezabezpečené podobě, lze klíč odchytit a následné šifrování komunikace SRTP pakety mohou být dešifrovány útočníkem. Právě proto se vyvinulo rozšíření RTP protokolu v podobě ZRTP, který se stará právě o zabezpečený přenos klíčů mezi účastníky hovoru pomocí Deffie-Hellmanova algoritmu. Při prvním spojení účastníků se proti útoku MiTM (man in the middle) ZRTP chrání tím, že vytvoří SAS (Short Authentication String), do kterého vloží vypočítaný hash z DH klíče a ten pošle pomocí ZRTP druhé straně, která také spočítá hash, a pokud se obě shodují, komunikace nebyla narušena útočníkem. Při dalších spojení účastníků se využívají klíče použité v předchozích hovorech a smíchávají je s klíči v dalších hovorech, tudíž je útok MiTM nerealizovatelný. [13]

Implementaci ZRTP může obsahovat přímo VoIP klient či může podporovat program Zfone. Zfone musíme nainstalovat jak u volajícího tak u volaného. Jeho funkce spočívá ve sledování paketů před jejich odesláním pomocí síťového rozhraní. Pokud detekuje RTP paket, vytvoří SRTP, tedy zašifrovaný RTP paket a zařadí zpátky do fronty paketů k odeslání. Poté na přijímací straně se spuštěným Zfone klientem se detekují pakety SRTP, které se dešifrují. [13]

3.3 Asterisk vůči síťovým útokům

U VoIP ústředny musíme zajistit zabezpečení proti síťovým útokům z důvodu dostupnosti ústředny pro klienty, které spojuje v realném čase. Zabezpečení ústředny vyžaduje od síťových administrátorů analýzu, plánování a realizaci potřebného opatření proti útokům. Nejdříve se seznámíme s nejčastějšími typy útoků a poté navrhneme proti nim zabezpečení.

3.3.1 DoS útok

Denial of service (DoS) je útok na specifickou službu a její zahlcení (flooding) nebo využití chyby (exploitation), falešnými zprávami či velkým množstvím zpráv. Typ útoku flooding je možné vytvořit na jakékoliv vrstvě TCP/IP, např. SYN flooding, který využívá three-way handshake. Útočník vytvoří paket TCP SYN a pošle serveru, který musí potvrdit paketem SYN-AK a čeká až mu i protistrana pošle SYN-AK. Pokud ho nepošle do určité doby, server znovu posílá SYN-AK, a toto se opakuje, dokud protistrana taky nepošle SYN-AK. Útočník má poté dvě možnosti: neodpovídat na SYN-AK nebo podstrčit falešnou IP adresu. Napadená služba je přetížena velkým přísunem žádostí a její odezva na další úkoly rapidně klesá nebo v horším případě neodpovídá. Příklad DoS útoku typu exploitation na telefonní přístoj VoIP je UDP paket větší než 65534 bajtů na port 5060, na kterém očekává zařízení SIP zprávy. Při takovém útoku telefonní zařízení přestane pracovat. [16] [17]

3.3.2 DDoS útok

Server, na němž běží PBX ústředna Asterisk, je limitován např. maximálním počtem obsloužených hovorů či připojením do internetu. DDoS se oproti DoS útoku liší tím, že není pouze jeden útočník, ale většinou skupina počítačů, tzv. botnet. Botnet nejčastěji vzniká napadením počítače virem (worm), který se rozesílá dále a vyčkává na pokyn od útočníka a poté zahájí útok. Jelikož server může být záplatovaný proti SYN paketům a na jednoho či pár útočníků může být imunní, ale ne proti tisícům. [17]

3.3.3 Port sken

Na internetu najdeme spoustu programů na skenování portů. To představuje nebezpečí skenování portů nejčastěji využívaných portů ve VoIP (SIP - 5060, IAX - 4569), kdy útočník si skenováním zjistí, na jakém serveru dané služby běží a poté zkouší cílené útoky. [17]

3.3.4 Přetečení zásobníku

Útok typu přetečení vyrovnávací paměti využívá vstupního parametru nebo chyby v softwaru. Vstupní parametr je několikrát větší než je očekávaná hodnota a ústředna může na něj zareagovat přetečením vyrovnávací paměti, toto má za následek výpadku služby. Například SIP zpráva INVITE může obsahovat prázdné hlavičky, neznámá záhlaví polí, parametry bez hodnoty, atd. [17]

3.3.5 Password Theft/Guessing

Heslo bývá často nejslabším článkem celého zabezpečení, jelikož ho vymýšlí člověk. Je důležité vytvořit pravidla pro heslo, a tím definovat složitost hesla (malá/velká písmena, znaky, číslice) a jeho délku. Nemělo by obsahovat celé slovo, ale náhodný řetězec, protože útočníci často používají útoky typu brutal-force nebo pomocí slovníku. [17]

3.3.6 Ochrana proti útokům

Proti výše popsaným DoS/DDoS útokům se bráníme nejčastěji správně nakonfigurovaným firewallem na perimetru sítě. Ten při větším množství paketů směřujících do sítě je nepustí do vnitřní sítě. Další možný způsob zabezpečení proti síťovým útokům je rozdělení fyzické sítě do logických segmentů, tzv. vlany. Tím docílíme toho, že lokální útočník ochromí pouze jeden segment sítě a ostatní segmenty nebudou útokem postiženi.

Při použití hubu v síti dochází k velkému vytížení celé sítě, protože jakýkoliv příchozí paket přeposílají na všechny porty, a tak se doporučuje vyměnit tyto prvky sítě za switche, které pakety přeposílají na daný port podle jejich MAC tabulky. Další možností je nasazení do sítě IPS (Intrusion Prevention System), který přijímá veškeré pakety, které prověří a pokud vyhodnotí paket zaslaný od útočníka, zahodí ho. Pokud používáme šifrování na všech zařízeních, mělo by se vypnout přijímání neautentizovaných zpráv. Chyby v softwaru a přetečení vyrovnávací paměti řešíme pomocí záplat či aktualizací firmware. Při útoku skenem portů využívá útočník znalost defaultních portů pro dané služby. To můžeme narušit tím, že zvolíme jiné rozsahy či čísla portů.

4 PRAKTICKÁ ČÁST

4.1 Instalace VoIP ústředny Asterisk

V říjnu 2010 vyšla verze 1.8 ústředny Asterisk [36], která je neustále aktualizována a poslední dostupná je verze 1.8.4.1. Instalaci ústředny Asterisk lze provádět dvěma způsoby. První je nechat balíčkovací systém `apt` automaticky nainstalovat a nebo si manuálně stáhnout balíčky a ústřednu, kterou si je možno modifikovat ke své potřebě. Nepotřebné balíčky neinstalovat, a tím nezvyšovat zátěž i paměťovou náročnost ústředny. Popisována bude druhá varianta. Pro popsání instalace balíčků a ústředny Asterisk bylo čerpáno ze zdrojů [31] a [32].

4.1.1 Potřebné balíčky pro Asterisk

Dříve než se pustíme do instalace ústředny je nutné mít nainstalované knihovny, které ústředna využívá. Asterisk byl nainstalován na linuxovou distribuci Ubuntu server 11.04 [35], který využívá balíčkovací systém `apt` stejně jako Debian. Jedná se o balíčky, které budeme potřebovat ke zkompilování ústředny a podpoře XML. Balíček build-essential obsahuje potřebné nástroje pro kompilaci – make, a kompilátory jazyka C (gcc) a C++ (g++).

```
apt-get install build-essential libxml2-dev ncurses-dev
```

4.1.2 Balíčky pro Jabber a LDAP

Doplněk res_jabber pro ústřednu Asterisk vyžaduje balíčky iksemel a openssl. Balíček openssl je už nainstalován při instalaci Ubuntu serveru, takže zbývá pouze iksemel, který slouží jako XML knihovna pro jabber. Server Ejabberd využívá certifikáty a Asterisk pro spojení potřebuje balíček `libssl-dev`. Balíček `openldap-dev` je z důvodu podpory databáze LDAP ústřednou Asterisk. Instalace se provádí pomocí apt-get viz příkaz níže.

```
apt-get install libiksemel-dev libldap2-dev libssl-dev
```

4.1.3 Balíčky pro H.323

Pro zprovoznění doplňku H.323 v ústředně Asterisk je třeba provést 3 kroky. Nejdříve je potřeba nainstalovat pomocí `apt-get` balíčky flex a bison.

```
apt-get install flex bison
cd /usr/include/linux
touch compiler.h
```

Druhým krokem je nainstalovat knihovnu PWlib, kterou vyžaduje openh323. Tato knihovna je multi-platformní a obsahuje části kódů, jež využívají jiné programy.

```
cd /usr/src
wget http://kent.dl.sourceforge.net/sourceforge/\
openh323/pwlib-v1_10_0-src-tar.gz
tar zxvf pwlib-v1_10_0-src-tar.gz
cd pwlib_v1_10_0/
./configure && make && make opt && make install
PWLIBDIR=/usr/src/pwlib_v1_10_0 && export PWLIBDIR
```

Posledním krokem je instalace balíčku openh323, která je obdobná jako ta předešlá. Úspěšně dokončenou instalaci je možné zkontrolovat v menuconfigu ústředny Asterisk, kde bude doplněk chan_h323 zaškrtnutý k instalaci.

```
cd /usr/src
wget http://ovh.dl.sourceforge.net/sourceforge/\
openh323/openh323-v1_18_0-src-tar.gz
tar zxvf openh323-v1_18_0-src-tar.gz
cd openh323_v1_18_0/
./configure && make && make opt && make install
OPENH323DIR=/usr/src/openh323_v1_18_0/ && export OPENH323DIR
echo "/usr/local/lib" >> /etc/ld.so.conf && ldconfig
```

4.1.4 Ústředna Asterisk

Instalace ústředny Asterisk je podobná té minulé s jedinou odlišností. Příkazem `make menuconfig` se spustí nabídka, kde volíme námi preferované součásti, které budou instalovány spolu s ústřednou. Například lze zvolit signalizační protokoly SIP, H.323, IAX nebo Skinny, dále podporované kodeky apod. Při instalaci ústředny byly zvoleny následující balíčky res_jabber, res_config_ldap a chan_h323. Příkaz `make samples` je volitelný, vytváří pouze ukázkové šablony konfiguračních souborů.

```
cd /usr/src
wget http://downloads.asterisk.org/pub/\
telephony/asterisk/asterisk-1.8-current.tar.gz
tar xvfz asterisk-1.8-current.tar.gz
cd asterisk-1.8.4.1/
./configure
make menuconfig
make && make install && make samples
```

4.2 Přesměrování hovorů

4.2.1 Pomocí ústředny

Ústřednou Asterisk a jejího číslovacího plánu lze realizovat přesměrování hovoru. Číslovací plán se skládá ze 3 částí. První je číslo klapky v našem případě je to 1000. Další číslo značí prioritu daného příkazu, nejvyšší prioritu má nejnižší číslo. Poslední částí je funkce, která má být uskutečněna. Vysvětlení uvedeného příkladu je následující. Pokud ústředna zaznamená žádost o hovor na číslo 1000, v první řadě vytáčí uživatele tomas po dobu 20s. Pokud uživatel tomas již hovoří či nepřijmul hovor, ústředna zareaguje další položkou s nižší prioritou, kterou je volání uživateli milan.

```
exten => 1000,1,Dial(SIP/tomas,20)
exten => 1000,2,Dial(SIP/martin,20)
```

4.2.2 Pomocí klienta Jitsi

Přesměrování probíhajícího hovoru lze provést pomocí klienta Jitsi [29]. Ten má tuto vlastnost zabudovanou a při hovoru stačí využít funkci přenést hovor, kam následně zadáme číslo, na které chceme hovor přesměrovat. Princip této funkce je odeslání SIP zprávy volajícímu metody REFER, kde informujeme pomocí položky REFER-To, kam se má hovor směrovat a položka Referred-By značí, komu tuto informaci podáváme. Volající, jakmile přijme zprávu, pak odešle volanému SIP zprávu 202 Accepted.

Obr. 4.1: Přesměrování hovoru pomocí klienta Jitsi

4.3 Překlad mezi protokoly SIP-SKYPE

VoIP ústředna Asterisk standartně neumí směrovat hovory na Skype. Řešení tohoto problému řeší například komerční Skype doplněk od firmy Digium, která vyvíjí i Asterisk. Spočívá nainstalováním balíčku `skypeforasterisk` a spuštěním knihovny `chan_skype`. Poté nadefinování číslovacího plánu pro příchozí a odchozí hovory. Další možností realizace hovorů SIP-SKYPE je pomocí Skype connect. Ten přiřadí skype účtu sip účet s číslem, které spravuje sip ústředna sip.skype.com.

V této práci byl zvolen nekomerční produkt SiSky, který vyžaduje instalaci SiSky brány, přes kterou jsou směrovány hovory na Skype. Při konfiguraci SiSky nelze využívat připojení ke vzdálené ploše, jelikož přesměrovává zvukové data ke vzdálenému klientovi, a tím znemožňuje správné funkci skype klientů, které využívá SiSky brána. Je tedy doporučeno použít VNC. Při konfiguraci SiSky brány bylo čerpáno z návodu [33].

4.3.1 Konfigurace SiSky brány

Program SiSkyEE byl nainstalován na počítač s operačním systémem Windows XP. Po nainstalování a spuštění SiSky brány byla provedena prvotní konfigurace, při které byl zadán počet trunk linek. Jedná se o skype účty a jejich počet závisí na počtu uživatelů, využívající ústřednu a počtu odchozích hovorů na Skype. Byly zvoleny 2 trunk linky, první pro extension (telefonní klapka) a druhou jako trunk linku.

Při konfiguraci první Skype trunk linky bylo zvoleno Works as Asterisk/IPPBX Extension. Zadáno

- User ID – 501 (SIP účet)
- Heslo – 501
- SIP proxy – 192.168.1.1 (IP adresa Asterisku)
- SIP domain – 192.168.1.1 (IP adresa Asterisku)

Stejné User ID a heslo bude definováno v konfiguračním souboru `sip.conf` a využíváno v číslovacím plánu. U druhé Skype trunk linky bylo zvoleno Works as Asterisk/IPPBX Trunk, a zadáno

- User ID – 901
- Heslo – 901

4.3.2 Správa SiSky brány

Při volbě Manage byl spuštěn prohlížeč s webovou administrací SiSky brány. V záložce Port bylo definováno u první linky položka Direct In. Tato volba určuje číslo, na které budou přesměrovány všechny hovory ze SKYPE-SIP při volání na první Skype trunk typu extension. Na další záložce User byla zapnuta volba Multi-user Mode a vytvořen uživatel. PIN slouží k identifikaci telefonního čísla pro SiSky bránu. Na záložce Phonebooku přiřazujeme čísla našim Skype kontaktům.

4.3.3 Konfigurace ústředny

Konfigurační soubor sip.conf

V konfiguračním souboru byla přidána trunk linka přidáním jednoho řádku pod sekci general. Hodnoty se shodují s definovanými v SiSky bráně.

```
register=901:901@192.168.1.2/901 ;SIP_ID:heslo@IP sisky_brány/SIP_ID
```

Poté byl přidán SIP účet pro extension a trunk linku vytvořenou v SiSky, viz příloha `sip.conf`. Správně definované účty si je možno ověřit v CLI Asterisku zadáním příkazu `sip show registry` či konfiguračním okně SiSky brány.

```
asteriskBP*CLI> sip show registry
Host                                    dnsmgr Username       Refresh State
192.168.1.2:5060                        N      901                105 Registered
1 SIP registrations.
asteriskBP*CLI>
```

Obr. 4.2: Ověření registrace trunk linky

Konfigurační soubor extensions.conf

Konfigurace číslovacího plánu spočívá ve vytvořením příchozích a odchozích pravidel pro hovory. Bylo definováno odchozí pravidlo pro skype trunk linku. Při vytočení čísla, kdy první číslo je 7, se hovor směruje na skype trunk linku, která se postará o směrování hovoru na skype.

```
exten => _7.,1,Dial(SIP/${EXTEN:1}@sip_trunk_901,30,r)
exten => _7.,n,Hangup
```

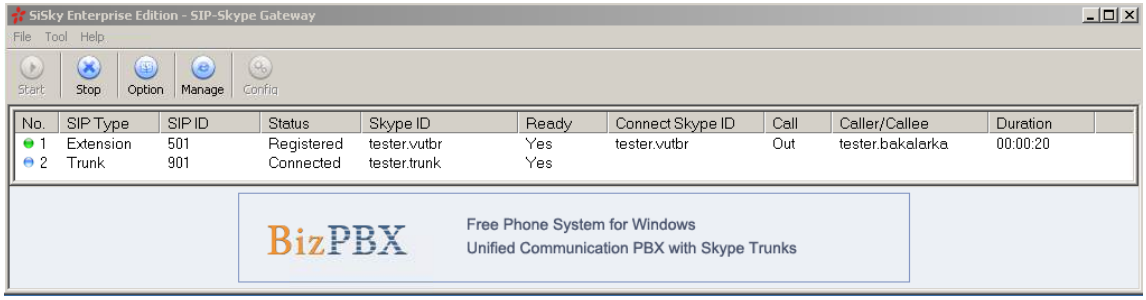
Druhé odchozí pravidlo definuje, že při vytočení čísla s počátečními číslicemi 50 či 501 je směrován hovor na skype extension.

```
exten => _50.,1,Dial(SIP/${EXTEN:0}@501)
exten => _501.,1,Dial(SIP/${EXTEN:0}@501)
```

Následující konfigurace v číslovacím plánu nám udává, že příchozí hovor na skype trunk linku bude směrován na SIP účet operator.

```
exten => 901,1,Dial(SIP/operator,20)
exten => 901,n,Hangup
```

Při správném nakonfigurování SiSky brány a ústředny Asterisk, jsme o hovorech ze SIP účtu na Skype v základním okně SiSky brány viz obrázek 4.3.



Obr. 4.3: SiSky brána při odchozím hovoru

4.4 Překlad mezi protokoly SIP-H.323

Překlad hovorů mezi signalizačními protokoly byl proveden pomocí číslovacího plánu. U verze ústředny Asterisk 1.8.4.1 je u chan_h323 bug (https://issues.asterisk.org/view.php?id=18670), který způsobuje nenavázání RTP spojení mezi hovořícími. Signalizace proběhla, ale při přijmutí hovoru ústředna spadla. U verze ústředny 1.6.2.18 se bug taky vyskytuje, ale u verze 1.4.41 se spojení naváže a RTP spojení mezi hovořícími funguje.

```
exten => 1002,2,Dial(H323/192.168.1.3,20)
```

4.5 Integrace LDAP

LDAP je adresářový server, který definuje uživatele, zařazuje je do stromové struktury a přiřazuje jim práva. Integraci LDAP do Asterisku je vhodné využít z důvodu centralizované správy uživatelů. Bylo využíváno návodu [19].

4.5.1 Instalace a konfigurace LDAP

Instalace LDAP serveru byla provedena na stejném serveru, kde běží ústředna Asterisk. Server byl zařazen v doméně testing.local. Ke zprovoznění LDAP serveru bylo zapotřebí 2 balíčků, a to `slapd` (LDAP server) a `ldap-utils` (pro jeho správu). Při průběhu instalace jsme byli vyzváni k vytvoření hesla k účtu admin.testing.local. Poté bylo nahráno schéma struktury definovanou Asteriskem. LDAP resetování pro její načtení. Soubor LDIF značí pro data k aktualizaci LDAP serveru.

```
apt-get install slapd ldap-utils
cp /usr/src/asterisk-1.8.4.1/contrib/scripts/asterisk.ldap-schema
/etc/ldap/schema/asterisk.schema

/etc/init.d/slapd restart
ldapadd -Y EXTERNAL -H ldapi:///
-f /usr/src/asterisk-1.8.4.1/contrib/scripts/asterisk.ldif
```

Uživatelé byli zařazeni do organizační skupiny people v doméně testing.local, proto byl vytvořen aktualizační soubor frontend.testing.local.ldif. Příkazem ldapadd byl vložen soubor do adresářového serveru.

```
dn: ou=people,dc=testing,dc=local
objectClass: organizationalUnit
ou: people

ldapadd -x -D cn=admin,dc=testing,dc=local -W
-f frontend.testing.local.ldif
```

Přidání uživatele do adresářové struktury se provádí taktéž pomocí souboru typu ldif. Rozsáhlejší nastavení naleznete v literatuře [19]. V této práci bude rozebráno pouze to důležité pro Asterisk. První řádek definuje zařazení uživatele ldapuser do námi vytvořené organizační skupiny. Userpassword je heslo uživatele uložené pomocí hash algoritmu MD5. Pro vytvoření hashe našeho hesla byl použit příkaz `echo "heslo"| md5sum`. Položka cn označuje jméno uživatele a parametry začínající AstAcount označují stejné příkazy jako jsou v `sip.conf`. Přehled všech parametrů nalezneme v souboru `extconfig.cfg`.

```
dn: uid=ldapuser,ou=people,dc=testing,dc=local
userPassword: {md5}1ff957bcca0b12c686d3b25bf46ea3b2
cn: ldapuser
AstAccountType: friend
AstAccountHost: dynamic
AstAccountContext: local
```

Vytvořený soubor byl vložen do adresářového serveru LDAP příkazem `ldapadd -x -D cn=admin,dc=testing,dc=local -f astuser.ldif -W`, ve které jsme byli tázáni na heslo k LDAP serveru. Další uživatelé se přidávají obdobným způsobem.

4.5.2 Konfigurace ústředny

Bylo nutné zvolit v konfiguračním souboru `sip.conf` parametr `rtcachefriends=yes` z důvodu real-time přidávání a odebírání uživatelů bez potřeby resetování ústředny. Dále byl upraven konfigurační soubor `extconfig.conf`, kde byla přidána databáze LDAP do správy seznamů uživatelů.

```
sipusers => ldap,"ou=people,dc=testing,dc=local",sip
sippeers => ldap,"ou=people,dc=testing,dc=local",sip
```

Poslední úpravy byly provedeny v `res_ldap.conf`, kde se definovaly informace o LDAP serveru.

```
[_general]
url=ldap://127.0.0.1:389          ;ip adresa:port - LDAP serveru
protocol=3                        ;verze protokolu LDAP
basedn=dc=testing,dc=local        ;domena
user=cn=admin,dc=testing,dc=local ;admin domeny
pass=heslo                        ;heslo k LDAP
```

4.6 Oznámení příchozího hovoru pomocí XMPP

XMPP je open source projekt pro instant messaging. Asterisk pro posílání zpráv pomocí protokolu xmpp/jabber potřebuje balíček res_jabber a spojení s jabber serverem. Jako jabber server nám poslouží ejabberd [34], který je taktéž open source a je dostupný ve verzích pro windows, linux či mac. Při konfigurace ústředny bylo použito návodu [25].

4.6.1 Konfigurace ejabberd

Ejabberd server byl nainstalován na počítač s operačním systémem Windows XP. Při instalaci bylo požadováno zadání domény, ve které se server nachází (testing.local). Při spuštění ejabberd serveru se spustil prohlížeč, ve kterém bylo zvoleno Admin interface a přihlášeno pomocí účtu vytvořeného při instalaci. V nabídce Virtual host byl zvolen hostitel. Poté se přešlo na záložku Uživatelé a byli vytvořeni 2 uživatelé. První bude sloužit pro ústřednu a druhý pro klienta, kterému budou zasílány zprávy o hovorech.

4.6.2 Konfigurace ústředny Asterisk

Nejprve byl upraven konfigurační soubor `jabber.conf`. Následující konfigurace byla vložena na konec souboru. Definuje spojení s ejabberd serverem, přihlášení uživatele, přes kterého budou zprávy odesílány.

```
[asterisk]                          ;nazev spojeni
type=client                         ;typ pripojeni
serverhost=192.168.1.2              ;adresa serveru ejabberd
username=asterisk@testing.local     ;uzivatelske jmeno
secret=heslo                        ;heslo
port=5222                           ;Port ejabberd serveru
```

Do konfiguračního souboru pro číslovací plán `extensions.conf` byl vložen následující řádek využívající příkaz `JABBERSend`, za kterým následuje odesílatel, příjemce, text zprávy. Příkaz se vkládá ke kontaktu, u kterého chceme býti informováni pomocí xmpp o příchozím hovoru. Příkaz je pro jeho délku zde rozdělen na 3 řádky, ale v konfiguračním souboru musí být pouze na jediném řádku.

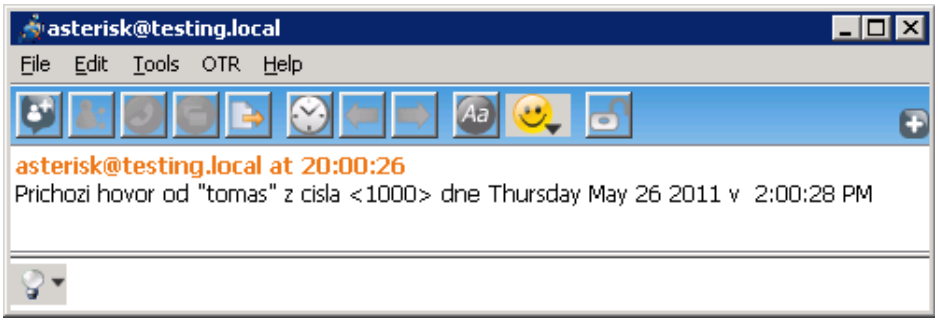
```
exten => 159,1,JABBERSend(asterisk,operator@testing.local
,Prichozi hovor od "${CALLERID(name)}" z cisla <${CALLERID(num)}>
dne ${STRFTIME(,EST5EDT,%A %B %d %G v %l:%M:%S %p)} )
```

4.6.3 Konfigurace klienta

Klientů pracující s protokolem XMPP je spousty, většina klientů je však multiprotokolová, a tak byl použit program Jitsi [29], dříve využívaný pro měření šířky pásma při použití video kodeků. Při nastavení klienta bylo zadáno

- Uživatelské jméno – operator@testing.local
- Heslo – heslo
- IP adresa ejabberd serveru – 192.168.1.2

Po správném zadání údajů klient byl připojen k serveru a označen jako online. Nyní již je schopný přijímat zprávy od Asterisku, který mu zasílá zprávy o příchozích hovorech.



Obr. 4.4: Zpráva o příchozím hovoru v programu Jitsi

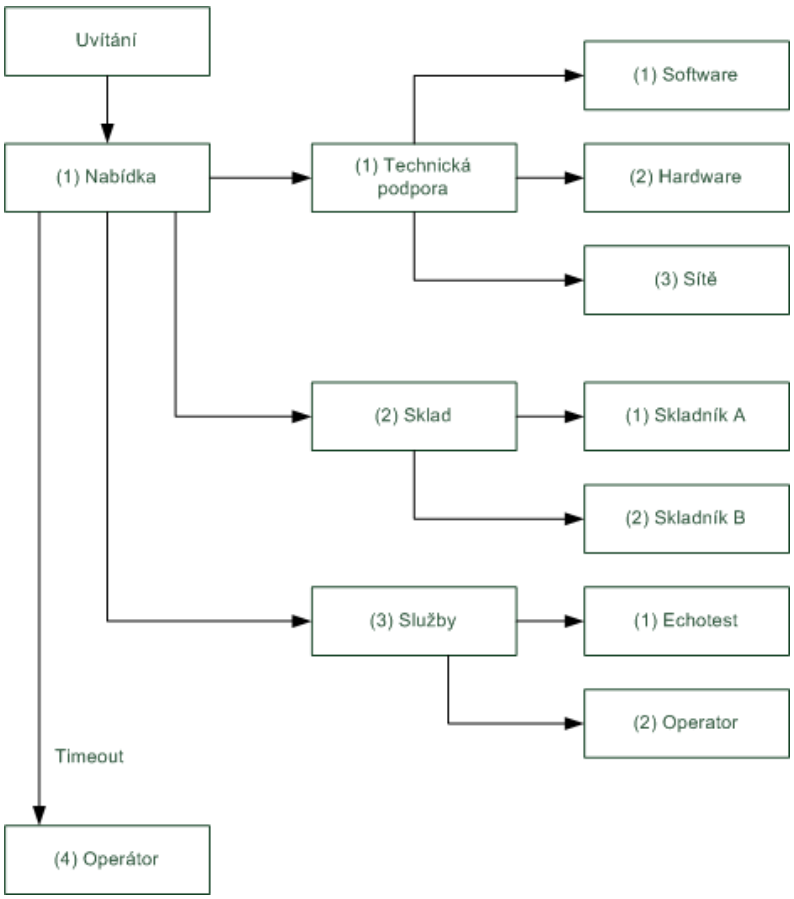
4.7 Vytvoření dialplanu s IVR

Interaktivní hlasový systém se využívá pro přesměrování hovoru dle požadavků volajícího. Ten svůj požadavek sděluje ústředně číselnou volbou (DMTF signály), kterou volí podle nastaveného číslovacího plánu (přepínání mezi kontexty), jenž využívá IVR. [25] [26] [27]

U kontextů jsou 4 možné parametry za příkazem `exten`.

- s – startovací, jsou v ní nejčastěji uvedeny možnosti, na které poté ústředna přesměruje volajícího
- i – byla zvolena neexistující možnost v ústředně
- t – vypršela doba pro zadání volby
- číslo – slouží pro vykonání žádosti, spouští aplikace (např. echo či volání) nebo slouží pro pohyb v menu IVR

V rámci této práce byl vytvořen IVR automat, jehož schéma je zobrazeno na obrázku 4.5. Konfigurace `extensions.conf` je uvedena v příloze na straně 61.



Obr. 4.5: Schéma IVR

4.8 Kodeky

Původně se slovo kodek skládal ze dvou kodér/dekodér, v dnešní době se spíše skládá z komprese/dekomprese. Kodeky využívají různé matematické modely, kterými snižují velikost přenášených dat. Tyto modely korespondují s lidským sluchem, který není dokonalý, a proto ty informace, které není schopen rozeznat, buď zcela odstraní či výrazně potlačí. Kodeky existují neztrátové nebo ztrátové. Jak už z názvů vypovídá, neztrátové kodeky uchovávají veškeré informace a jsou i přenášeny ty, které člověk nemusí slyšet, tzv. nadbytečné data. Ztrátové kodeky odebírají informace, které můžeme či nemůžeme slyšet. Čím větší ztráta informací, tím menší šířka pásma a naopak. [19]

4.8.1 Popis audio kodeků

G.711

Nejstarší a nejrozšířenější kodek, který byl používán v PSTN. Pokud je ústředna Asterisk spojena i s telefonní sítí, je vhodné povolit tento kodek. Existují dvě verze kodeku G.711 – a-law a μ-law. G.711 μ-law se používá v Americe a Japonsku využívá rozlišení pouze 7 bitové a zbylý 1 bit využívá k signalizaci, a-law v Evropě. Při volání s odlišným typem kodeku G.711 musí dojít k překódování, protože μ-law využívá větší kompresi. V telefonních sítích se používá vzorkovací frekvence 8 kHz s rozlišením 8 bitů. Vynásobením těchto hodnot získáme šířku pásma 64 kb/s. Kodek G.711 je nenáročný na procesor, jelikož je téměř neztrátový. Ztrátu způsobuje pouze companding, což zvyšuje odstup signálu od šumu, odstraňuje šustění či dýchání. [19] [21]

G.722

Kodek G.722 vznikl jako standard organizace ITU-T a zabírá šířku pásma 48, 56 nebo 64 kb/s. Využívá ADPCM modulaci, která nepopisuje získané hodnoty, ale pouze rozdíl aktuální hodnoty od té předchozí. Vzorkovací frekvence je 8 kHz pro zachování zpětné kompatibility. Lze použít 16 kHz frekvenci pro zvýšení kvality přenášeného zvuku. [22]

G.726

Standard G.726 vytvořila organizace ITU-T stejně jako G.722 a jedná se o rozšířený kodek z důvodu nízké náročnosti na výkon zařízení. Využívá ADPCM, která způsobuje, že při šířce pásma 32 kb/s dokáže přenášet audio informace kvalitativně

srovnatelné s G.711 s šířkou pásma 64 kb/s. Ústředna Asterisk využívá G.726 se šířkou pásma 32 kb/s (další jsou 16 kb/s či 24 kb/s). [19] [20]

GSM

Původní název GSM kodeku byl RPE-LTP (Regular Pulse Excitation Long-Term Prediction), byl navržen pro mobilní komunikaci, tudíž musí splňovat nízké nároky na výpočetní výkon, ale nabízí i nízkou šířku pásma 13 kb/s. Princip kodeku je rozdělit signál na bloky po 20 ms, které se kódují na rámce o velikosti 260 bitů. Kodek GSM využívá i informace z předchozích bloků. [19] [20]

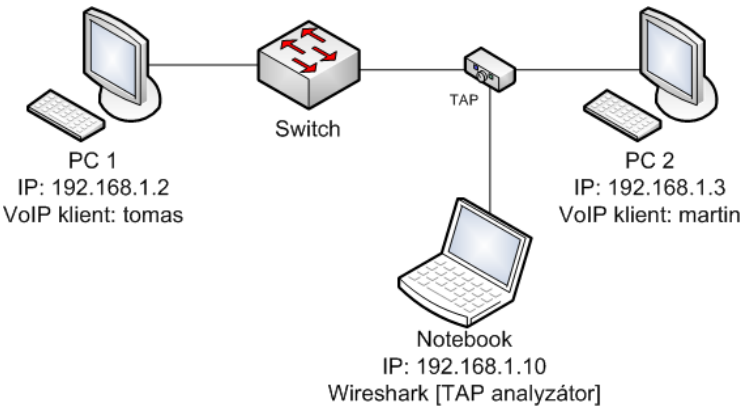
iLBC

Internet Low Bitrate Codec vychází z principu, kdy hlasový signál je porovnáván s databází hlasů. Tímto vznikne velice nenáročný kodek se šířkou pásma 13, 3 kb/s nebo 15, 2 kb/s. Nevýhodou kodeku je audio výstup robotického charakteru.[19] [20]

Speex

Speex kodek je jako jediný z výše definovaných kodeků s proměnnou šířkou pásma 2,15-22,4 kb/s, v závislosti na požadavcích hovoru. Speex je možné přizpůsobit svým potřebám, ale jeho nevýhodou je náročnost na výpočetní výkon.[19] [20]

4.8.2 Měření závislosti šířky pásma audio kodeky



Obr. 4.6: Schéma sítě při měření kodeků

K měření využití šířky pásma byl použit program Wireshark [30]. Ten získával pakety pomocí síťového analyzátoru TAP LE-580FX, který byl vložen mezi dva počítače s operačním systémem Windows 7 se softwarovými telefony Phonerlite

v1.81 [28] viz schéma sítě na obrázku 4.6. U nich bylo zapnuto zahazování prázdných RTP paketů. Zvuk byl přiváděn na vstup zvukové karty pomocí mp3 přehrávače, který přehrával stejný záznam u všech provedených měření. Jednalo se o monolog s mluveným slovem. Měření bylo provedeno bez použití ústředny Asterisk, hovor byl spojen peer-to-peer a trval 126 sekund.

Tab. 4.1: RTP měření audio kodeků

Název kodeku	**Počet RTP paketů**	**RTP paket [B]**	**Dat.tok [kb/s]**
G.711 a-law	9364	214	127,22
G.711 μ-law	9163	214	124,49
G.722	9403	214	127,76
G.726-16	9454	94	56,43
G.726-24	9467	114	68,52
G.726-32	9631	134	81,94
G.726-40	9625	154	94,11
GSM	9660	87	53,36
iLBC	9499	92	55,49
Speex	12541	86	67,80
Speex WB	12515	96	75,55

Tab. 4.2: SRTP měření audio kodeků

Název kodeku	**Počet RTP paketů**	**RTP paket [B]**	**Dat. tok [kb/s]**
G.711 a-law	9878	224	140,49
G.711 μ-law	8687	224	123,55
G.722	8893	224	126,48
G.726-16	9671	104	63,86
G.726-24	9314	124	73,33
G.726-32	8615	144	78,77
G.726-40	9644	164	100,42
GSM	9072	97	55,87
iLBC	9872	102	63,94
Speex	12534	94	74,08
Speex WB	13125	105	86,80

V tabulce 4.3 je uveden celkový objem přenesených RTP dat naměřený pomocí Wiresharku a rozdíl v procentech mezi nešifrovanou a nešifrovanou komunikací.

Tab. 4.3: Srovnání náročnosti na šířku pásma u audio kodeků

Název kodeku	RTP [kB]	SRTP [kB]	Rozdíl [%]
G.711 a-law	2004	2213	10,43
G.711 μ-law	1961	1946	−0,76
G.722	2013	1992	−1,00
G.726-16	889	1006	13,17
G.726-24	1080	1155	7,02
G.726-32	1291	1241	−3,87
G.726-40	1483	1582	6,70
GSM	841	880	4,70
iLBC	874	1007	15,23
Speex	1068	1167	9,27
Speex WB	1190	1368	14,89

4.8.3 Popis video kodeků

H.263

Kodek H.263 byl navržen pro videokonference s nízkou šířkou pásma s konstantní přenosovou rychlostí. Vytvořila ho organizace ITU-T, v roce 1995 byla první verze tohoto kodeku. Další vylepšení přišlo v roce 1998 (H.263v2) a 2000 (H.263v3), kdy se přidávaly další funkce. Kodek pracuje s modelem YCbCr a vzorkováním 4:2:0. Podporuje rozlišení o velikostech od 128x96 až do 1408x1152 při 29,97 snímcích za sekundu. [6] [23]

H.264/MPEG4 AVC

Na jeho vývoji spolupracovaly dvě organizace ITU a ISO/IEC a každá ho pojmenovala jinak, proto má dva názvy H.264 nebo MPEG4 část 10 (AVC). Oproti H.263 dosahuje lepších výsledků při stejné kvalitě, a to 30 až 50 % šířky pásma. To je ovšem vykoupeno 4-násobně větší náročností na výpočetní výkon při kódování a 3 násobně při dekódování. Využívá několik profilů s nastavením komprimace obrazu a pro videokonference se používá základní. [6]

Theora

Theora je open source kodek, který vytvořila Xiph.org nadace. Rozlišení videa může až do HD rozlišení 1920x1080. Svoji kvalitou je na úrovni MPEG4 a pro zvuk využívá Vorbis kodek. [24]

4.8.4 Měření závislosti šířky pásma video kodeky

K měření šířky pásma při přenosu videohovorů bylo použito Wiresharku [30], který získával data od zařízení TAP LE-580FX. Ten byl stejně jako u měření audio kodeků mezi počítači viz schéma sítě obrázek 4.6, ale s operačním systémem Ubuntu 11.04 [35] s webovými kamerami Logitech QuickCam Communicate STX. Softwarový klient byl použit program Jitsi [29], který umí 2 video kodeky – H.263-1998 a H.264 s nastaveným rozlišení 640x480 s 30 snímky za sekundu. U kodeku H.263-1998 se při hovoru rozlišení změnilo od nastaveného 640x480 na 176x144, což vysvětluje tak nízkou šířku pásma oproti ostatním kodekům. Pro šifrování hovorů využívá program Jitsi protokol ZRTP. Dále byly změřeny pomocí programu Linphone [37] kodeky – H.263, H.263-1998, MP4-ES a Theora. Měření probíhalo při rozlišení 800x600.

Tab. 4.4: RTP měření video kodeků

Program	**Jitsi**		**Linphone**			
Kodek	H.263-1998	H.264	H.263	H.263-1998	MP4V-ES	Theora
RTP paketů	4776	13499	32460	26336	19101	12644
Doba hovoru[s]	114,263	119,297	120,515	120,211	120,315	121,669
Celkem dat [KB]	3527	14229	32275	31809	26129	16835
Dat. tok [Mb/s]	0,247	0,954	2,142	2,217	1,737	1,107

Tab. 4.5: ZRTP měření video kodeků

Program	**Jitsi**	
Kodek	H.263-1998	H.264
RTP paketů	4706	13604
Doba hovoru [s]	114,347	119,084
Celkem dat [KB]	3471	14414
Dat. tok [Mb/s]	0,243	0,968
Rozdíl [%]	-1,62	1,28

5 ZÁVĚR

Tato bakalářská práce se zabývá signalizačními protokoly, přenosem hovorových dat a PBX ústřednou Asterisk. Jsou popsány architektury v signalizačních protokolech a vysvětleny různé principy navázání spojení, pomocí nejčastěji používaných signalizačních protokolů. Dále je popsán protokol RTP, který přenáší multimediální data.

Definováno je zabezpečení u signalizačních protokolů. U protokolu H.323 je to pomocí profilů, které se liší různými druhy a silou zabezpečení. Využívají symetrických klíčů, hashovacího algoritmu MD5 či SHA1 nebo pomocí certifikátů. U SIP protokolu je uvažováno taktéž několik možných variant zabezpečení. Jelikož je SIP podobný HTTP, je u něj použita HTTP autentizace, která se ale nedoporučuje, jelikož je autentizace přenášena buď nezašifrovaně nebo pomocí MD5, která byla už prolomena. Silnější ochrana pomocí S/MINE využívající certifikátů snižuje výkon, a tím zvyšuje zpoždění. Dalšími možnostmi jsou IPsec či TLS. U protokolu IAX, přenášejícího signalizační i multimediální data, je vše šifrováno nativně pomocí 128-bitového šifrovacího algoritmu AES.

K přenosu multimediálních dat u protokolů H.323 a SIP se využívá RTP protokol. Rozšířením RTP o zabezpečení je protokol SRTP, který využívá hashovací funkce k autentizaci hlavičky paketu a šifrovacího algoritmu AES k ochraně multimediálních dat.

V další části jsou zmíněny nejčastější útoky na PBX ústřednu Asterisk. Některé formy útoků lze vyřešit správným nakonfigurováním aktivních prvků v síti. Proti ostatním útokům se bráníme pomocí záplatování či změnou konfigurace ústředny.

V praktické části byla popsána instalace ústředny Asterisk s balíčky potřebnými pro rozšiřující funkce. K přesměrování dosud nenavázaných spojení bylo vyřešeno pomocí dialplanu a již navázaných spojení pomocí softwarového klienta Jitsi. V dialplanu byl i nakonfigurován ukázkový IVR automat. Řeší vstupy od uživatele a má strukturu dělenou na oddělení technické podpory, skladu a služeb.

Překlad SIP-SKYPE byl splněn pomocí nekomerčního řešení SiSky brány. Byla popsána konfigurace a správa brány. Brána slouží k propojení SIP sítě s SKYPE pomocí Skype klientů. Nevýhodou toho řešení je nutnost použití grafického rozhraní pro spuštění Skype klientů. Překlad mezi protokoly SIP-H.323 byl vyřešen pomocí dialplanu. Signalizaci hovorů ústředna vytvořila, ale RTP spojení u verze vyšší než 1.4 nefungovalo. Tato chyba je nahlášena jako bug.

Integraci s adresářovým serverem LDAP byla docílena externí správa uživatelů. Tímto řešením lze vytvořit uživatele, kdy jeden účet slouží k přihlášení k linuxovému počítači, emailové poště a VoIP ústředně.

Pro využívání protokolu XMPP bylo zapotřebí vytvořit Jabber server. Ten byl

nakonfigurován a byli vytvořeni dva uživatelé. Jeden pro ústřednu a jeden jako klient, na který byly zasílány zprávy o hovorech.

Při měření audio kodeků bylo zjištěno, že rozdíl mezi nešifrovanou a šifrovanou komunikací se pohybuje v rozmezí od -4% do 15%. Tento rozdíl ovlivňuje použitý kodek než použité šifrování AES, který využívá protokol SRTP. Při měření video kodeků byl rozdíl mezi nešifrovanou a šifrovanou komunikací $\pm$ 2%.

LITERATURA

[1] KUMAR, Vineet; KORPI, Markku; SENGODAN, Senthil. *IP Telephony With H.323 : Architectuer for Unified Networks and Intergrated Services.* Wiley Computer Publishing, 2001. 605 s. ISBN 0-471-39343-6.

[2] International Telecommunication Union. *Packetizer [online]. 2009 [cit. 2010-11-24]. H.323 Standards.* Dostupné z URL: <http://www.packetizer.com/ipmc/h323/standards.html>.

[3] Network Working Group. *IETF [online]. 2002 [cit. 2010-11-24]. SIP: Session Initiation Protocol.* Dostupné z URL: <http://www.ietf.org/rfc/rfc3261.txt>.

[4] Session Initiation Protocol. *In Wikipedia : the free encyclopedia [online].* St. Petersburg (Florida) : Wikipedia Foundation, 8.5.2006, last modified on 13.11.2010 [cit. 2010-11-24]. Dostupné z URL: <http://cs.wikipedia.org/wiki/Session_Initiation_Protocol>.

[5] SINNREICH, Henry; JOHNSTON, Alan B. *Internet Communications Using SIP.* Canada : Wiley Publishing, Inc., 2006. 377 s. ISBN 978-0-471-77657-4.

[6] FIRESTONE, Scott; RAMALINGAM, Thiya; FRY, Steve. *Voice and Video Conferencing Fundamentals.* USA : Cisco Press, 2007. 376 s. ISBN 978-1-58705-268-2.

[7] DAVIDSON, Johnathan, et al. *Voice over IP Fundamentals, Second Edition.* USA : Cisco Press, 2006. 432 s. ISBN 978-1-58705-257-6.

[8] The Internet Engineering Task Force [online]. *IAX: Inter-Asterisk eXchange Version 2. February 2010 [cit. 2010-12-06].* Dostupné z URL: <http://tools.ietf.org/search/rfc5456>.

[9] VOZŇÁK PH.D, Ing. Miroslav. Cesnet [online]. Listopad 2008 [cit. 2010-12-06]. *TELEFONNÍ ÚSTŘEDNY ASTERISK.* Dostupné z URL: <http://www.iptelefon.cz/archiv/dok_osta/ipt-2008_Telefonni_ustredny_Asterisk.pdf>.

[10] WIJA, Tomáš; ZUKAL, David; VOZŇÁK, Miroslav. Cesnet [online]. 30.10.2005 [cit. 2010-12-06]. *Asterisk a jeho použití.* Dostupné z URL: <http://www.cesnet.cz/akce/20051115/pr/voz05_asterisk.pdf>.

[11] ČERVENKA, Marek. Root.cz [online]. 18.11.2010 [cit. 2010-12-06]. *Asterisk 1.8 už není jen telefonní ústředna.* Dostupné z URL: <http://www.root.cz/clanky/asterisk-1-8-uz-neni-jen-telefonni-ustredna/>.

[12] MEGGELEN, Jim Van; MADSEN, Leif; SMITH, Jared. *Asterisk : The Future of Telephony, Second Edition [online].* United States of America : O´Reilly Media, 2007 [cit. 2010-12-06]. Dostupné z URL: <http://cdn.oreilly.com/books/9780596510480.pdf>. ISBN 978-0-596-51048-0.

[13] DWIVEDI, Himanshu. *VoIP - Protocols, Attacks, and Countermeasures.* USA : No Starch Press , 2009. 211 s. ISBN 978-1-59327-163-3.

[14] The Internet Engineering Task Force [online]. March 2004 [cit. 2010-12-06]. *The Secure Real-time Transport Protocol (SRTP).* Dostupné z URL: <http://www.ietf.org/rfc/rfc3711.txt>.

[15] KUHN, D. Richard; WALSH, Thomas J.; FRIES, Steffen. National Initute of Standards and Technology [online]. January 2005 [cit. 2010-12-06]. *Security Considerations for Voice Over IP Systems.* Dostupné z URL: <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>.

[16] PORTER, Thomas; GOUGH, Michael. *How to cheat at VoIP Security.* United States of America : Syngress Publishing, 2007. 412 s. ISBN 978-1-59749-169-3.

[17] JOHNSTON, Alan B.; PISCITELLO, David M. *Understanding Voice over IP Security.* USA : Artech House, 2006. 261 s. ISBN 1-59693-050-0.

[18] BOUCADAIR, M. *Inter-Asterisk Exchange (IAX): Deployment Scenarios in SIP-Enabled Networks.* John Wiley & Sons Ltd., 2009. 272 s. ISBN: 978-0-470-77072-6.

[19] MADSEN, Leif; MEGGELEN, Jim Van; BRYANT, Russell. *Asterisk : The Definitive Guide. 3rd Edition.* USA : O´Reilly Media, 2011. 736 s. ISBN 978-0-596-51734-2.

[20] Voip-info.org [online]. 2011 [cit. 2011-05-18]. *Voip-info.org.* Dostupné z WWW: <voip-info.org>.

[21] *G.711. In Wikipedia : the free encyclopedia [online].* St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 21.4.2011 [cit. 2011-05-18]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/G.711>.

[22] *G.722. In Wikipedia : the free encyclopedia [online].* St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 10.12.2010 [cit. 2011-05-18]. Dostupné z WWW: <http://en.wikipedia.org/wiki/G.722>.

[23] *H.263. In Wikipedia : the free encyclopedia [online].* St. Petersburg (Florida) : Wikipedia Foundation, , last modified on 4.3.2011 [cit. 2011-05-19]. Dostupné z WWW: <http://en.wikipedia.org/wiki/H.263>.

[24] *Theora, video for everyone [online].* 2011 [cit. 2011-05-19]. Theora.org :: main. Dostupné z WWW: <http://www.theora.org>.

[25] GIBSON, Matthew. *Voip Phreak* [online]. 2008 [cit. 2011-05-27]. VOIP News, Tutorials, Reviews and More from Voip Phreak. Dostupné z WWW: <http://www.voipphreak.ca/wp-content/uploads/2008/01/ast_xmpp_article.pdf>.

[26] ŠILHAVÝ, Pavel; KRAJSA, Ondřej; DANĚČEK, Vít. *MTIS* [online]. 2011 [cit. 2011-05-27]. MTIS. Dostupné z WWW: <http://anca.utko.feec.vutbr.cz/vyuka_data/mtis/Lab3.pdf>.

[27] BINDER, Tomáš. *Správa a konfigurace VoIP ústředny Asterisk* [online]. Brno : VUT v Brně, 2007. 60 s. Diplomová práce. VUT v Brně. Dostupné z WWW: <https://www.vutbr.cz/studium/zaverecne-prace?zp_id=14185>.

[28] *PhonerLite* [online]. 2011 [cit. 2011-05-27]. Dostupný z WWW: <http://www.phonerlite.de/index en.htm>.

[29] *Jitsi (SIP Communicator)* [online]. 2011 [cit. 2011-05-27]. Dostupný z WWW: <http://www.jitsi.org/index.php/Main/HomePage>.

[30] *Wireshark* [online]. 2011 [cit. 2011-05-27]. Dostupný z WWW: <http://www.wireshark.org/>.

[31] *H323 installation* [online]. 2007 [cit. 2011-05-27]. On Debian and Asterisk 1.4. Dostupné z WWW: <http://www.voip-info.org/wiki/view/H323+installation+on+Debian+and+Asterisk+1.4>.

[32] *How to install Asterisk 1.8 on Ubuntu Server 11.04* [online]. May 5, 2011 [cit. 2011-05-27]. Let IT know. Dostupné z WWW: <http://letitknow.wordpress.com/2011/05/05/how-to-install-asterisk-1-8-on-ubuntu-server-11-04/>.

[33] *SiSkyEE* [online]. 2011 [cit. 2011-05-27]. Skype asterisk, skype asterisk, ip pbx skype, skype ippbx, skype trunk, skype pbx, sip skype, sip to skype, skype sip, skype to sip, skype call center, skype gateway, skype exchange. Dostupné z WWW: <http://www.yeastar.com/download/SiSky_UserManual.pdf>.

[34] *Ejabberd Community Site* [online]. 2011 [cit. 2011-05-28]. The Erlang Jabber/XMPP daemon. Dostupné z WWW: <http://www.ejabberd.im/>.

[35] *Www.ubuntu.cz* [online]. 2011 [cit. 2011-05-28]. Co je to Ubuntu?. Dostupné z WWW: <http://www.ubuntu.cz/>.

[36] *Asterisk* [online]. 2011 [cit. 2011-05-28]. The Open Source Telephony Projects. Dostupné z WWW: <http://www.asterisk.org/>.

[37] *Linphone, open-source voip software* [online]. 2011 [cit. 2011-05-28]. Linphone, an open-source video sip phone. Dostupné z WWW: <http://www.linphone.org/>.

SEZNAM SYMBOLŮ, VELIČIN A ZKRATEK

ACK Acknowledgement

AES Adavanced Encryption Standard

AVC Advanced Video Coding

AVT Audio/Video Transport

CA Certificate authority

DoS Denial of Service

DDoS Distributed Denial of Service

DTMF Dual Tone Multiple Frequency

FQDN Fully Qualified Domain Name

GPL General Public Licence

GRQ Gatekeeper request

HTTP HyperText Transport Protocol

IANA Internet Assigned Cumbers Authority

IAX/IAX2 Inter-Asterisk eXchange

IETF Internet Engineering Task Force

IKE Internet Key Exchange

IM Instant Message

IP Internet Protocol

IPS Intrusion Prevention Systems

ISO International Organization for Standardization

ITU International Telecommunications Union

ISAKMP Internet Security Association and Key Management Protocol

IVR Interactive Voice Response

LAN Local Area Network

LDAP Lightweight Directory Access Protocol

MCU Multipoint Control Unit

MIME Multipurpose Internet Mail Extensions

MiTM Man in the middle

MPEG Motion Picture Experts Group

PBX Private Branch Exchange

PSTN Public Switched Telephone Network

QoS Quality of Service

RFC Request for comments

RTCP RTP Control Protocol

RTP Real-Time Transport Protocol

SAS Short Authentication String

SIP Session Initiation Protocol

SHA Secure Hash Algorithm

S/MIME Secure Multipurpose Inteent Mail Extensions

SMTP Simple Mail Transport Protocol

TCP Transmission Control Protocol

TDM Time-Division Multiplex

UA User Agent

UDP User Datagram Protocol

VLAN Virtual LAN

VNC Virtual Network Computing

VoIP Voice over Internet Protocol

VPN Virtual Private Network

XMPP Extensible Messaging and Presence Protocol

SEZNAM PŘÍLOH

A KONFIGURAČNÍ SOUBORY

A.1 sip.conf

```
[general]
register=901:901@192.168.1.2/901
rtcachefriends=yes
;language=cz

;local

[sip_trunk_901]
username=901
type=friend
secret=901
nat=yes
insecure=very
host=192.168.1.2
fromuser=901
fromdomain=192.168.1.2
dtmfmode=rfc2833
context=from-trunk
canreinvite=no
qualify=yes
disallow=all
allow=ulaw
allow=alaw
allow=gsm
;allow=g729
allow=ilbc

[501]
type=friend
secret=501
qualify=yes
nat=no
host=dynamic
canreinvite=no
```

```
context=local

[tomas]
type=friend
callerid="tomas" <1000>
host=dynamic
secret=heslo
context=local

[martin]

type=friend
callerid="martin" <1001>
host=dynamic
secret=heslo
context=local

[operator]
type=friend
callerid="operator" <159>
host=dynamic
secret=heslo
context=local

;technicka_podpora

[software]
type=friend
callerid="software" <2000>
host=dynamic
secret=heslo
context=tech_podpora

[hardware]
type=friend
callerid="hardware" <2001>
host=dynamic
secret=heslo
context=tech_podpora
```

```
[site]
type=friend
callerid="site" <2002>
host=dynamic
secret=heslo
context=tech_podpora

;sklad

[skladnik_a]
type=friend
callerid="skladnik_a" <3000>
host=dynamic
secret=heslo
context=sklad

[skladnik_b]
type=friend
callerid="skladnik_b" <3001>
host=dynamic
secret=heslo
context=sklad
```

A.2 extensions.conf

```
[local]
exten => _7.,1,Dial(SIP/${EXTEN:1}@sip_trunk_901,30,r)
exten => _7.,n,Hangup

exten => _50.,1,Dial(SIP/${EXTEN:0}@501)
exten => _501.,1,Dial(SIP/${EXTEN:0}@501)

exten => 159,1,Dial(SIP/operator,20)
exten => 1000,1,Dial(SIP/tomas,20)
exten => 1000,2,Dial(SIP/martin,20)
exten => 1001,1,Dial(SIP/martin,20)
exten => 1002,1,Dial(H323/192.168.1.3,20)
```

```
exten => 1010,1,Goto(mainmenu,s,1)

[mainmenu]
exten => s,1,Set(POLOHA=0)
exten => s,2,Playback(uvitani)
exten => s,3(start),Background(moznosti_menu)
exten => s,n,WaitExten(10)

;mozne volby
exten => 1,1,Goto(tech_podpora,s,1)
exten => 2,1,Goto(sklad,s,1)
exten => 3,1,Goto(sluzby,s,1)
exten => 4,1,Goto(operator,s,1)

;pri spatne volbe
exten => i,1,Playback(spatnavolba)
exten => i,n,Set(POLOHA=0)
exten => i,n,Wait(2)
exten => i,n,Goto(mainmenu,s,3)

;pri vyprseni timeout, ci 3x zadane spatne volbe
exten => t,1,Set(POLOHA=$[${POLOHA} + 1])
exten => t,2,GotoIf($[ ${POLOHA} >= 3]?operator,s,1)
exten => t,3,Playback(spatnavolba)
exten => t,n,Wait(2)
exten => t,n,Goto(mainmenu,s,3)

[tech_podpora]
exten => s,1,Background(moznosti_tech)
exten => s,n,WaitExten(10)
exten => i,1,Goto(tech_podpora,s,1)
exten => t,1,Goto(mainmenu,s,3)

exten => 1,1,Dial(SIP/software,20)
exten => 2,1,Dial(SIP/hardware,20)
exten => 3,1,Dial(SIP/site,20)

[sklad]
exten => s,1,Background(moznosti_sklad)
```

```
exten => s,n,WaitExten(10)
exten => i,1,Goto(sklad,s,1)
exten => t,1,Goto(mainmenu,s,3)

exten => 1,1,Dial(SIP/skladnik_a,20)
exten => 2,1,Dial(SIP/skladnik_b,20)

[sluzby]
exten => s,1,Background(moznosti_sluzby)
exten => s,n,WaitExten(10)
exten => i,1,Goto(sluzby,s,1)
exten => t,1,Goto(mainmenu,s,3)

;Echo test
exten => 1,1,Playback(demo-echotest)
exten => 1,2,Echo
exten => 1,3,Playback(demo-echodone)
exten => 1,4,Goto(mainmenu,s,start)

;operator
exten => 2,1,Goto(operator,s,1)

[operator]
exten => s,1,JABBERSend(asterisk,operator@testing.local,Prichozi hovor
od "${CALLERID(name)}" z cisla <${CALLERID(num)}> dne
${STRFTIME(,EST5EDT,%A %B %d %G v %l:%M:%S %p)} )
exten => s,2,Dial(SIP/operator,20)

[from-trunk]
exten => 901,1,Dial(SIP/operator,20)
exten => 901,n,Hangup
```

B PŘILOŽENÉ CD

- Bakalářská práce v elektronické podobě pdf
- Konfigurační soubory
- Použitá nahrávka při měření audio kodeků
- Print screen konfigurací
- Wireshark soubory ve formátu pcap